Tribunal Superior Eleitoral

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TESTES PÚBLICOS DE SEGURANÇA DA URNA ELETRÔNICA

Compêndio

Brasília – 2016

Tribunal Superior Eleitoral

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Compêndio

Brasília – 2016

Secretaria de Gestão da Informação
SAFS, Quadra 7, Lotes 1/2
70070-600 – Brasília/DF
Telefone: (61) 3030-9225

Secretário-Geral da Presidência
Carlos Vieira von Adamek

Diretora-Geral da Secretaria
Leda Marlene Bandeira

Secretário de Gestão da Informação
Geraldo Campetti Sobrinho

Unidade responsável
Comissão Reguladora do TPS 2016

Editoração e revisão editorial
Coordenadoria de Editoração e Publicações (Cedip/SGI)

Editoração
Seção de Editoração e Programação Visual (Seprov/Cedip/SGI)

Capa e projeto gráfico
Rauf Soares

Revisão editorial
Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGI)

Impressão e acabamento
Seção de Impressão e Distribuição (Segraf/Cedip/SGI)

Dados Internacionais de Catalogação na Publicação (CIP)
(Tribunal Superior Eleitoral – Biblioteca Prof. Alysson Darowish Mitraud)

Brasil. Tribunal Superior Eleitoral.

Teste público de segurança 2016 do sistema público de votação : compêndio.-- Brasília : Tribunal Superior Eleitoral, 2016

157 p. : Il. ; 23 cm.

Unidade responsável: Comissão Reguladora do TPS 2016.

1. Votação – teste público de segurança - Brasil. 2. Urna eletrônica – segurança - Brasil. 3. Segurança do voto na urna eletrônica – Brasil. I. Título

CDD 324.665
CDDir 341.28435

Tribunal Superior Eleitoral

Presidente
Ministro Dias Toffoli

Vice-Presidente
Ministro Gilmar Mendes

Ministros Efetivos
Ministro Luiz Fux
Ministra Maria Thereza de Assis Moura
Ministro Herman Benjamin
Ministro Henrique Neves
Ministra Luciana Lóssio

Procurador-Geral Eleitoral
Rodrigo Janot Monteiro de Barros

Sumário

Apresentação

O momento de votação é o ponto basilar da democracia brasileira, em que cada cidadão, em pleno exercício de seus direitos políticos, pode manifestar sua opinião para a escolha de seus representantes, em um processo eleitoral que alcança mais de 140 milhões de pessoas.

Por meio da urna eletrônica, o eleitor exercita a sua cidadania. Com vistas ao aprimoramento dos aspectos relativos à segurança da informação, transparência e confiabilidade do processo eleitoral brasileiro, o Tribunal Superior Eleitoral submete os seus sistemas ao Teste Público de Segurança (TPS).

Em 2016 foi realizado, na sede do Tribunal Superior Eleitoral, o terceiro Teste Público de Segurança. Este relatório contempla toda a documentação produzida durante os testes, dentre elas, as conclusões da Comissão Avaliadora.

Comissão Reguladora do TPS 2016

1. Introdução

O Teste Público de Segurança (TPS), evento inédito no mundo, foi criado por iniciativa do Tribunal Superior Eleitoral (TSE), com o objetivo de fortalecer a confiabilidade, a transparência, a segurança da captação e da apuração dos votos, bem como de propiciar melhorias contínuas no processo eleitoral brasileiro.

Pautado na transparência institucional – um dos pilares de atuação do TSE e de toda a Justiça Eleitoral brasileira –, o teste reúne especialistas em Tecnologia e Segurança da Informação de diversas organizações, instituições acadêmicas e órgãos públicos. Na ocasião, os participantes tentam atacar a urna e seus componentes internos e externos, com o objetivo de descobrir vulnerabilidades do sistema com relação à possibilidade de violação de resultados e quebra do sigilo do voto.

A terceira edição do Teste Público de Segurança ocorreu durante os dias 8, 9 e 10 de março de 2016, no edifício-sede do TSE, em Brasília. O espaço foi preparado exclusivamente para o evento, com entrada controlada e ambiente monitorado por câmeras. Participaram do evento 13 investigadores, os quais tiveram acesso aos componentes internos e externos do sistema eletrônico de votação para criarem seus planos de ataque.

Os participantes estavam divididos em quatro grupos, sendo apenas uma inscrição individual. Eles apresentaram, ao todo, oito propostas de planos de ataque. As propostas buscaram quebrar o sigilo do voto e/ou fraudar a destinação dos votos registrados na urna.

A primeira edição do Teste foi realizada do dia 10 a 13 de novembro de 2009. Durante os quatro dias, os participantes tentaram violar os sistemas, sem sucesso. Não foi detectada qualquer falha nas barreiras de proteção contra fraudes e tentativas de violação.

A segunda edição ocorreu entre os dias 20 e 22 de março de 2012, quando foi detectada a necessidade de fortalecer a aleatoriedade da sequência dos votos a fim de evitar a identificação da ordem de registro dos votos, o que foi realizado imediatamente após a descoberta do problema. A não conformidade estava relacionada ao algoritmo de embaralhamento dos votos no RDV (Registro Digital do Voto), ou seja, à ordem de gravação dos votos de cada eleitor.

No total das duas edições (de 2009 e de 2012), foram executados 27 planos de ataques, com as mais engenhosas ideias, todas sem sucesso. Essas experiências foram, entretanto, extremamente positivas, pois deram ao TSE a chance de aperfeiçoar a segurança e aumentar a confiabilidade dos sistemas, a partir das análises e conclusões feitas pelos investigadores, o que incentivou a continuação da iniciativa em eleições posteriores.

Em 30 de abril de 2015, o Plenário do TSE aprovou a Resolução nº 23.444, que institucionalizou a realização periódica do Teste Público de Segurança durante o ciclo de desenvolvimento dos sistemas de votação e apuração, constituindo, obrigatoriamente, parte integrante do processo eleitoral brasileiro.

A realização dos Testes Públicos de Segurança decorre da confiança da Justiça Eleitoral na maturidade e qualidade dos sistemas eleitorais. A medida não consta de nenhum instrumento normativo; é uma iniciativa da própria JE, com o objetivo de fortalecer cada vez mais o processo eleitoral, colocando-o à prova para a comunidade e reunindo especialistas de universidades, instituições de pesquisa e estudiosos de todo o Brasil para contribuírem com a segurança das urnas e do voto.

2. O Teste Público de Segurança

O Teste Público de Segurança constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, apuração, transmissão e recebimento de arquivos, e deve ser realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

Presidido pelo próprio presidente do TSE, o TPS ocorre em evento aberto à participação da sociedade, com o objetivo de fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral, contemplando ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Os sistemas eleitorais que são objetos de investigação do Teste Público de Segurança são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados.

2.1 Normas reguladoras

A Resolução nº 23.444/2015 (Anexo A) foi publicada com o objetivo de instituir a realização periódica do TPS no ciclo de desenvolvimento dos sistemas de votação e apuração e permanece a principal norma sobre o tema, definindo-o como parte integrante do processo eleitoral brasileiro, devendo ser realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais. A resolução também indica a elaboração de edital específico para a realização das edições do teste.

No dia 1º de dezembro de 2015 foi publicado o Edital do Teste Público de Segurança 2016 (Anexo A), contemplando as regras específicas e datas para a realização de todas as demais fases e ações do TPS. O edital foi debatido com a sociedade e as contribuições dos cidadãos contribuíram para o texto final do edital.

2.2 Comissões

A Resolução-TSE nº 23.444/2015 definiu a atuação e as atribuições de quatro comissões: Comissão Organizadora, Comissão Reguladora, Comissão Avaliadora e Comissão de Comunicação Institucional, cujas composições estão no Anexo B.

Destaca-se, dentre elas, a Comissão Avaliadora, cuja composição se dá por: um representante indicado pelo ministro presidente do TSE; membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação; um representante do Ministério Público Federal; um representante da Ordem dos Advogados do Brasil; um representante do Congresso Nacional; um perito criminal federal da área de Informática, do Departamento de Polícia Federal; um engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (Crea), indicado pelo Conselho Federal de Engenharia e Agronomia (Confea); e um representante da Sociedade Brasileira de Computação (SBC). Essa comissão pode, ainda, valer-se de integrantes do TSE para assessorá-los.

A principal função dessa comissão foi avaliar e homologar os resultados obtidos no evento e produzir um relatório final conclusivo (Anexo G). Nesse relatório, foram registradas as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às possíveis fraudes identificadas durante o TPS.

2.3 Participação

Puderam participar do TPS 2016, na condição de técnico(s) e/ou de grupo(s) de técnicos, cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, que preenchessem os requisitos definidos no edital (Anexo A), que limitou a quantidade máxima de participantes a 25 pessoas, somando-se as participações individuais e em grupo, podendo cada equipe conter de dois a cinco membros. Também foi estabelecido o limite de 20 inscrições possíveis, isto é, a soma do número de grupos de investigadores e de investigadores individuais não poderia ultrapassar dez.

Foi vedada a participação de membros das comissões e de pessoas com mais de uma inscrição, seja em grupo ou individual.

2.4 Etapas

O Teste Público de Segurança foi dividido – seguindo o definido no art.17 da Resolução-TSE nº 23.444/2015 – nas fases de preparação, realização e avaliação.

a. Preparação

A fase de preparação consistiu no período em que os investigadores e/ou grupos de investigadores puderam configurar os sistemas que utilizariam no teste e elaborar

seu plano de testes. Foi realizada audiência pública, com o objetivo de esclarecer as regras do TPS. A Justiça Eleitoral também promoveu palestra informativa sobre o sistema eletrônico de votação, que subsidiou os participantes sobre o funcionamento do sistema eleitoral. Ainda nessa fase, ocorreu a publicação do edital com as regras específicas e datas para a realização de todas as demais fases e ações do evento.

Foi disponibilizado local para a visualização do código-fonte em um ambiente controlado e segregado ao da realização do TPS. O acesso ao código só pôde ser realizado mediante assinatura de um termo de confidencialidade pelos grupos e investigadores individuais, tendo sido vedada a extração, impressão e/ou reprodução, mesmo que parcial, do código-fonte e vedado ingressar no ambiente segregado ao da realização dos testes com qualquer instrumento que permitisse a cópia do código-fonte. Foram permitidas apenas anotações que não confrontassem o termo de confidencialidade. Na fase de preparação, também foram preparados e configurados os sistemas adicionais que foram utilizados no teste.

A solicitação para participação no evento foi dividida em duas etapas. Na primeira, de pré-inscrição, o candidato deveria preencher o formulário de pré-inscrição e enviá-lo ao TSE. Na segunda etapa, a inscrição em si foi realizada por meio do preenchimento de Plano de Teste, documento com o detalhamento de como se daria a tentativa de violação do sistema eletrônico de votação. O plano enviado pelos investigadores e grupos de investigadores que tiveram a pré-inscrição aprovada foram submetidos à Comissão Reguladora para avaliação.

O microcomputador disponibilizado pelo TSE, a urna eletrônica e os demais equipamentos foram lacrados ao término da fase de preparação. Esses equipamentos tiveram sua integridade verificada no dia do teste pelos investigadores e/ou grupo de investigadores e pelos componentes das comissões.

b. Realização

Na fase de realização, os técnicos com inscrições homologadas compareceram ao TSE para a realização do Teste Público de Segurança e realizaram os planos de teste previamente definidos, seguindo as regras definidas no edital.

Ao final da realização do TPS, cada investigador ou grupo de investigadores apresentou relatório das ações executadas e dos resultados alcançados.

Os investigadores ou grupos que identificassem alguma falha, vulnerabilidade explorada ou fraude no sistema eletrônico de votação deveriam, ao final, fazer sugestões de melhoria relacionadas aos erros encontrados.

c. Avaliação

Na fase de avaliação, a Comissão Avaliadora, elaborou relatório de avaliação (Anexo G) contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas durante o TPS.

3. Seleção de projetos

Para que os planos de testes fossem aprovados, os investigadores precisaram atender as exigências estipuladas no parágrafo único do art. 20 do Edital do Teste Público de segurança 2016, sendo motivo de reprovação o não cumprimento dos requisitos abaixo relacionados, conforme o dispositivo mencionado:

I. não atenderem aos objetivos específicos de alterar a destinação dos votos ou fragilizar o sigilo do voto;

II. não atenderem ao objeto estabelecido no edital[1];

III. não demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou

IV. forem entregues após o prazo estipulado no Marco 7 do Calendário do Evento. (anexado ao final do Edital do Teste Público de Segurança, Anexo A).

O documento com a declaração dos inscritos aprovados e a avaliação dos planos de testes encontra-se no (Anexo C) deste compêndio.

3.1 Projetos avaliados

Após a avaliação dos planos de testes, quatro grupos de investigadores e um investigador individual foram classificados para participar do Teste Público de Segurança 2016. Oito planos foram aprovados, tendo quatro deles como objetivo quebrar o sigilo do voto e tendo os outros quatro, alterar a destinação dos votos.

Durante o evento, o investigador João Felipe submeteu à apreciação da Comissão Reguladora o plano de teste intitulado Sequenciador de Votos[2], que foi aprovado e executado, tendo obtido sucesso em dois ataques contidos em seu plano.

Em anexo (Anexo D), estão todos os planos de testes submetidos à Comissão Reguladora, dentre os quais, os aprovados e os reprovados durante o processo de avaliação, assim como aqueles submetidos durante a realização dos testes[3]. A seguir estão apenas os planos aprovados durante a fase de seleção.

[1] Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados.;

[2] Plano de teste submetido durante o evento e aceito pela Comissão Reguladora.

[3] Foi permitido aos participantes alterarem seus planos de testes e submeterem novos planos, os quais foram submetidos à nova aprovação da Comissão Reguladora, conforme previsto no art. 32, § 2º, do Edital do Teste Público de Segurança 2016.

Investigadores / grupo aprovado de investigadores	Resumo do plano de teste
Grupo 1	O teste proposto refere-se ao Sistema de Apuração (SA), especificamente, à funcionalidade identificada como Votação Totalmente Eletrônica, que permite a apuração por meio da digitação de um boletim de urna (BU). Essa operação ocorre como medida de contingência, por exemplo, nos casos de falhas em urna na qual não tenha sido possível a recuperação dos dados. Digitam-se, então, os dados dessa urna em uma nova, preparada com o SA.
Grupo 2	Tentativa de violar o sigilo do voto, capturando as comunicações realizadas entre o terminal do mesário e a urna.
Grupo 4	Tentativa de fraude na destinação dos votos na urna por meio de controle dos dispositivos de teclado e impressora.
Grupo 5	Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual.
Investigador individual: João Felipe Souza	Ataques: • Destruidor de votos: Teste para explorar o controle de transação da urna e destruir votos depois do registro de comparecimento dos eleitores. • *Reflash* da urna: Teste para explorar possível vulnerabilidade no processo de carga da urna e realizar eleições simuladas e direcionadas. • Registrador do teclado: Teste para quebrar o sigilo do voto introduzindo dispositivo para registro das teclas digitadas na urna eletrônica. • *Root kit* JE Connect: Teste para explorar possível vulnerabilidade no *kit* JE Connect e obter acesso ao RECArquivos e InfoArquivos.

4. Resultados

Embora a realização dos testes tenha ocorrido nos dias 8 e 10 de março de 2016, alguns investigadores, entretanto, optaram por comparecer ao TSE também no dia 7 de março, data prevista no calendário do evento para a preparação do ambiente de trabalho dos investigadores.

Após o término do evento, os membros da Comissão Avaliadora, de posse dos planos de testes e documentação de execução dos testes (Anexo F), reuniram-se para elaboração do relatório de avaliação dos testes públicos de segurança (Anexo G)[4].

No dia 15 de março, foi realizada no TSE audiência pública para divulgação dos resultados e das conclusões do Teste Público de Segurança. O Ministro Henrique Neves fez a leitura do relatório da Comissão Avaliadora.

4.1 Conclusões/Soluções a serem tomadas

Diante dos registros de falhas identificadas durante os testes e apresentadas no relatório da Comissão Avaliadora, o TSE convocará os investigadores para executarem novamente os mesmos testes, em uma nova versão do sistema eleitoral, em que terão sido feitas as devidas correções. Essa nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano de teste que identificou a falha, vulnerabilidade explorada ou fraude. O plano pode ser alterado somente em função das correções realizadas nos sistemas afetados.

4.2 Encerramento e certificação

Em 15 de março de 2016, durante a audiência pública com a finalidade de se divulgarem os resultados e as conclusões do TPS, foram entregues certificados de participação aos investigadores e grupos de investigadores.

Aqueles que não puderam comparecer à cerimônia, receberam o documento no endereço informado na inscrição. Segue abaixo lista de investigadores que obtiveram a certificação:

Grupo 1 – Sérgio Freitas da Silva

Grupo 2 – Charles Figueredo de Barros, Igor Carpanase Figueiredo

Grupo 4 – Elisabete Evaldt, Gustavo Henrique Cervi

Grupo 5 – Luis Fernando de Almeida, Jeferson Lesbão de Siqueira, Alison Luiz de Oliveira Chaves, Vinicius Zibetti Resko, Fabio Rosindo Daher de Barros

Investigador Individual: João Felipe Souza

[4] Nota da Comissão Avaliadora: o investigador João Felipe Souza teve sucesso em dois ataques, denominados *Reflash* de Urna e Sequenciador de Votos. Por equívoco, constou do relatório elaborado pela Comissão Avaliadora apenas a análise do ataque denominado Sequenciador de Votos, erroneamente intitulado naquele documento como *Reflash* de Urna.

Tribunal Superior Eleitoral

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Anexos

Anexo A – Normas para o Teste Público de Segurança 2016

Resolução-TSE n° 23.444/2015

Resolução nº 23.444, de 30 de abril de 2015 – Brasília – DF

Dispõe sobre a realização periódica do Teste Público de Segurança – TPS nos sistemas eleitorais que especifica.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das atribuições que lhe conferem o art. 23, IX, do Código Eleitoral e o art. 105 da Lei nº 9.504, de 30 de setembro de 1997, resolve expedir a seguinte instrução:

CAPÍTULO I

DO OBJETO

Art. 1º Fica instituído o Teste Público de Segurança TPS no ciclo de desenvolvimento dos sistemas de votação e apuração.

§ 1º O TPS de que trata esta resolução constitui parte integrante do processo eleitoral brasileiro e será realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

§ 2º A presidência dos trabalhos relativos ao TPS será exercida pelo Presidente do Tribunal Superior Eleitoral.

Art. 2º Os sistemas eleitorais que poderão ser objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, conforme definido no § 2º do art. 66 da Lei nº 9.504/1997, incluindo o *hardware* da urna e seus *softwares* embarcados.

CAPÍTULO II

DO OBJETIVO

Art. 3º O Teste Público de Segurança tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral.

Parágrafo único. O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

CAPÍTULO III

DAS DEFINIÇÕES

Art. 4º Para os fins desta resolução, considera-se:

I – Falha: evento em que se observa que um sistema violou sua especificação por ter entrado em um estado inconsistente ocasionado por uma imperfeição (defeito) em um *software* ou *hardware* impedindo seu bom funcionamento, sem interferir na destinação e/ou anonimato dos votos dos eleitores.

II – Vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas não seja condição suficiente para alcançar um dos objetivos definidos no parágrafo único do art. 3º.

III – Fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis.

IV – Plano de testes: documento que será fornecido para identificação e descrição das ações a serem desempenhadas pelo(s) técnico(s) e/ou grupo(s) de técnicos quando da realização do teste.

V – Ambiente de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para que o(s) técnico(s) e/ou o(s) grupo(s) de técnicos possam preparar e realizar os testes.

CAPÍTULO IV

DAS ATRIBUIÇÕES

Art. 5º As unidades do Tribunal Superior Eleitoral deverão atuar, observadas as respectivas atribuições, para a plena realização do teste instituído por esta resolução.

Art. 6º Atuarão no Teste Público de Segurança:

I – Comissão Organizadora;

II – Comissão Reguladora;

III – Comissão Avaliadora;

IV – Comissão de Comunicação Institucional.

Art. 7º A gerência geral da realização do TPS será feita por integrantes da Diretoria-Geral, designados por portaria do Presidente do Tribunal.

Art. 8º A Comissão Organizadora terá as seguintes atribuições:

I – planejar e elaborar o projeto geral para a realização do evento;

II – organizar e prover a infraestrutura necessária para a realização de todas as fases do TPS;

III – convocar as demais áreas do Tribunal, observadas as respectivas atribuições administrativas, a fim de providenciar ações ou infraestrutura para a realização do evento;

IV – manter informadas a Presidência e a Diretoria-Geral sobre o andamento dos trabalhos.

Parágrafo único. A Comissão Organizadora será composta pelas áreas da Diretoria-Geral, Administração, Segurança, Imprensa e Comunicação Social, Infraestrutura de TI e do Cerimonial.

Art. 9º A Comissão Reguladora terá as seguintes atribuições:

I – definir os procedimentos e a metodologia utilizados;

II – aprovar a(s) inscrição(ões) do(s) técnico(s) e/ou do(s) grupo(s) de técnicos que tenha(m) atendido às exigências constantes do edital;

III – supervisionar e documentar todas as fases do evento;

IV – aprovar os planos de testes elaborados pelo(s) técnico(s) e/ou grupo(s) de técnicos;

V – realizar outras atividades relacionadas à disciplina do TPS, visando ao fiel cumprimento do objetivo desta resolução, ressalvadas as atribuições das demais comissões e da Presidência do Tribunal Superior Eleitoral;

VI – elaborar, em conjunto com a Comissão Organizadora, a minuta do edital que disciplinará a convocação e as etapas do TPS.

Parágrafo único. Os componentes da Comissão de que trata o *caput* deste artigo serão indicados por portaria, entre os quais no mínimo um com conhecimentos jurídicos indicado pela Presidência do Tribunal, integrantes da Secretaria de Tecnologia da Informação e um integrante da Comissão de Comunicação Institucional, definida no art. 11 desta resolução.

Art. 10. A Comissão Avaliadora terá as seguintes atribuições:

I – validar a metodologia e os critérios de julgamento definidos pela Comissão Disciplinadora do Teste Público de Segurança;

II – avaliar e homologar os resultados obtidos e produzir relatório final conclusivo.

§ 1º A Comissão de que trata o *caput* deste artigo será nomeada pelo Presidente do Tribunal, com a seguinte composição:

I – um representante indicado pelo Ministro Presidente;

II – membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação;

III – um representante do Ministério Público Federal;

IV – um representante da Ordem dos Advogados do Brasil;

V – um representante do Congresso Nacional;

VI – um perito criminal federal da área de Informática, do Departamento de Polícia Federal;

VII – um engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (CREA), indicado pelo Conselho Federal de Engenharia e Agronomia (CONFEA);

VIII – um representante da Sociedade Brasileira de Computação (SBC).

§ 2º A Comissão poderá se valer de integrantes do Tribunal para assessorá-los.

§ 3º O Tribunal disponibilizará serviços de secretariado, espaço e infraestrutura à Comissão.

§ 4º Para a indicação dos integrantes definidos nos incisos III a VIII do § 1º deste artigo as respectivas instituições serão oficiadas para indicarem os componentes mencionados.

Art. 11. A Comissão de Comunicação Institucional terá as seguintes atribuições:

I – elaborar o plano de comunicação sobre o evento;

II – receber as solicitações de informação do público externo e centralizar a publicação de informações e notícias sobre o TPS, observadas as orientações da Presidência e da Diretoria-Geral;

III – responsabilizar-se pela cobertura jornalística do evento e credenciamento dos veículos de comunicação.

Parágrafo único. A Comissão de Comunicação Institucional será composta pelas áreas da Diretoria-Geral, Imprensa e Comunicação Social e Tecnologia da Informação.

CAPÍTULO V

DA PARTICIPAÇÃO

Art. 12. Poderão participar, na condição de técnico(s) e/ou de grupo(s) de técnicos, cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, que preencham os requisitos definidos em edital.

§ 1º O edital de que trata o *caput* disciplinará a quantidade máxima de participantes e equipes, bem como os critérios para inscrição, seleção e avaliação.

§ 2º Em caso de inscrições em quantidade superior à definida no edital de que trata o § 1º deste artigo, haverá sorteio público, entre as inscrições aprovadas.

Art. 13. É vedada a participação, na condição de técnico(s) e/ou grupo(s) de técnicos, de componentes das Comissões referidas no art. 6º desta resolução.

Art. 14. Para promover a participação no TPS, o(s) técnico(s) e/ou grupo(s) de técnicos que reside(m) fora do município de realização do evento poderá(ão) requerer passagens e diárias ao Tribunal Superior Eleitoral.

Parágrafo único. As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral, além daquelas estipuladas no respectivo edital.

Art. 15. Ao final da fase de realização do Teste Público de Segurança, cada técnico ou grupo de técnicos deverá apresentar Relatório Técnico das ações executadas e resultados alcançados, de acordo com as regras definidas em edital.

Art. 16. O(s) técnico(s) e/ou grupo(s) de técnicos, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, deverá(ão) apresentar a(s) respectiva(s) sugestão(ões) de melhoria.

§ 1º Em um prazo de até 6 (seis) meses após a realização do TPS, o(s) técnico(s) e/ou grupo(s) de técnicos poderá(ão) ser convocado(s) a executar novamente, em uma nova versão do sistema eleitoral com as devidas correções, os mesmos testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 2º A nova execução dos testes de que trata o parágrafo anterior não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas no sistema.

§ 3º Para o disposto no § 1º, as modificações realizadas serão apresentadas, observado o disposto no § 2º do artigo 18.

CAPÍTULO VI

DAS FASES DO TESTE PÚBLICO DE SEGURANÇA

Art. 17. O Teste Público de Segurança será dividido nas fases de preparação, realização e avaliação.

Art. 18. Na fase de preparação, deverão ser realizadas as seguintes ações ou eventos:

I – audiência pública com o objetivo de esclarecer as regras do TPS definidas nesta resolução;

II – publicação do edital que deverá contemplar as regras específicas e datas para a realização de todas as demais fases e ações do evento;

III – palestra informativa sobre o sistema eletrônico de votação com o objetivo de subsidiar os eventuais participantes sobre o funcionamento do sistema eleitoral;

IV – apresentação, em ambiente controlado, dos códigos-fonte dos sistemas eleitorais que farão parte do TPS;

V – geração de versão a ser utilizada no TPS, observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas;

VI – preparação e configuração dos sistemas adicionais que serão utilizados no teste e elaboração dos respectivos planos de teste;

VII – recebimento das inscrições e planos de teste dos técnicos que desejam participar do evento.

§ 1º Poderão ser definidas outras ações ou eventos intermediários para atender objetivos complementares desta fase, desde que estejam definidos no edital da respectiva edição do TPS.

§ 2º A apresentação dos códigos-fonte, de que trata o inciso IV deste artigo, será feita em ambiente controlado, com acesso mediante Termo de Confidencialidade e regras específicas definidas em edital.

Art. 19. Na fase de realização, os técnicos com inscrições homologadas comparecerão no local determinado para a realização do Teste Público de Segurança para executar no ambiente de teste os planos de teste previamente definidos, conforme regras definidas no edital.

Art. 20. Na fase de avaliação, a Comissão Avaliadora definida no art. 10, de posse dos planos de testes e documentação de execução dos testes, deverá elaborar relatório de avaliação contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas durante o TPS.

§ 1º O Tribunal promoverá evento de encerramento para demonstrar os resultados alcançados, que deverá contar com a presença do(s) técnico(s) e/ou grupo(s) de técnicos e Comissão Avaliadora.

§ 2º A Secretaria de Gestão da Informação será responsável por editar publicação específica, em formato físico e eletrônico, contendo um compêndio da documentação produzida e conclusões da Comissão Avaliadora.

§ 3º A publicação, em formato eletrônico, de que trata o parágrafo anterior deverá ser disponibilizada no sítio do Tribunal Superior Eleitoral.

CAPÍTULO VII

DAS DISPOSIÇÕES GERAIS

Art. 21. O edital que disciplinará cada edição do Teste Público de Segurança será publicado no *DJe*/TSE e divulgado no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 22. Será dada publicidade à composição das comissões descritas no art. 6º desta resolução no *DJe*/TSE e no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 23. Os participantes do TPS que tiverem a inscrição aprovada deverão manter conduta ética nas declarações e ilações sobre as hipóteses e resultados encontrados.

Art. 24. Fica autorizada a contratação e/ou celebração de convênio com instituições renomadas para realizar a pré-avaliação da segurança dos sistemas eleitorais e assessorar a realização do TPS.

Art. 25. O Tribunal Superior Eleitoral promoverá a criação de uma unidade ou núcleo permanente para tratar sistematicamente as questões relativas à segurança do processo eleitoral informatizado e à realização do teste de que cuida esta norma.

Art. 26. Os casos omissos serão dirimidos pela Presidência do Tribunal Superior Eleitoral.

Art. 27. Esta Resolução entra em vigor na data de sua publicação.

Brasília, 30 de abril de 2015.

Ministro DIAS TOFFOLI, presidente e relator – Ministro GILMAR MENDES – Ministro LUIZ FUX – Ministro JOÃO OTÁVIO DE NORONHA – Ministra MARIA THEREZA DE ASSIS MOURA – Ministro HENRIQUE NEVES DA SILVA – Ministro ADMAR GONZAGA.

Publicada no *DJE* de 21.5.2015.

Edital do Teste Público de Segurança 2016

TRIBUNAL SUPERIOR ELEITORAL

EDITAL DO TESTE PÚBLICO DE SEGURANÇA

A Comissão Reguladora comunica aos interessados que, conforme estabelecido na Resolução TSE nº 23.444, de 30 de abril de 2015, será realizado o Teste Público de Segurança no sistema eletrônico de votação, no período de 8 a 10 de março de 2016, de 9 a 18 horas, na sede do TSE (Setor de Administração Federal Sul – SAFS, Quadra 7, lotes 1/2, Brasília /DF).

CAPÍTULO I
DO OBJETO

Art. 1º Constitui objeto deste edital a realização do Teste Público de Segurança (TPS) no sistema eletrônico de votação que será utilizado nas eleições municipais de 2016.

Parágrafo único. O TPS de que trata este edital constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, apuração, transmissão e recebimento de arquivos.

Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados.

§ 1° Os componentes de *software* e *hardware* que serão objeto do TPS consistem em:

I – Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE);

1

II – *Software* Básico da Urna Eletrônica, *Software* de Carga (SCUE), Gerenciador de Aplicativos (GAP), *Software* de Votação (VOTA), Recuperador de Dados (RED) e Sistema de Apuração (SA);

III – Sistemas Transportador, RecArquivos e InfoArquivos;

IV – Subsistema de Instalação e Segurança (SIS) e Kit JE Connect;

V – Urna modelo 2013, com seus respectivos *firmwares* e mídias eletrônicas.

§ 2° Não serão objetos do TPS os seguintes sistemas, ambientes, procedimentos e elementos abaixo relacionados:

I – identificação e verificação biométrica do eleitor;

II – preparação e infraestrutura para o Kit JE Connect;

III – processamento dos arquivos de urna (fase prévia à totalização dos resultados e posterior às fases de transmissão e de recebimento dos arquivos gerados pela urna eletrônica após o encerramento da votação na seção);

IV – totalização (TOT) e gerenciamento da totalização (GER);

V – acesso às máquinas servidoras;

VI – acesso aos bancos de dados;

VII – ataques de negação de serviço;

VIII – ataque destrutivo à urna eletrônica e demais recursos computacionais da Justiça Eleitoral;

IX – sistema de geração de chaves criptográficas;

X – alteração do código-fonte dos sistemas;

XI – ambiente de compilação dos sistemas;

XII – lacre físico: selos autoadesivos utilizados na urna eletrônica com a finalidade de detectar eventuais violações ao equipamento; e

§ 3° Conforme o § 2º do artigo 66 da Lei 9.504, as chaves eletrônicas privadas e senhas eletrônicas de acesso manter-se-ão sob sigilo da Justiça Eleitoral.

§ 4° A versão dos sistemas a ser utilizada no TPS será gerada conforme observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas.

2

CAPÍTULO II
DO OBJETIVO

Art. 3º O Teste Público de Segurança tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar aperfeiçoamento do processo eleitoral.

Parágrafo único. O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição e apresentar as respectivas sugestões de melhoria.

CAPÍTULO III
DAS DEFINIÇÕES

Art. 4º Para fins deste edital, considera-se:

I – falha: evento em que se observa que um sistema violou sua especificação por ter entrado em um estado inconsistente ocasionado por uma imperfeição (defeito) em um *software* ou *hardware*, impedindo seu bom funcionamento, sem interferir na destinação e/ou anonimato dos votos dos eleitores.

II – vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas que não seja condição suficiente para violar a destinação ou sigilo dos votos, ou, caso sejam alcançados, que deixe a existência de vestígios.

III – fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis.

IV – plano de teste: documento que será fornecido para identificação e descrição das ações a serem desempenhadas pelos investigadores e/ou grupos de investigadores quando da realização do teste.

V – ambiente de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para

que os investigadores e/ou grupos de investigadores possam preparar e realizar os testes.

CAPÍTULO IV
DA COORDENAÇÃO E DA ATUAÇÃO NO TESTE PÚBLICO DE SEGURANÇA

Art. 5º O Teste Público de Segurança será coordenado pelo Ministro Presidente do TSE.

Art. 6º Conforme estabelecido no art. 6º da Resolução TSE nº 23.444, atuarão no Teste Público de Segurança:

I – Comissão Organizadora;

II – Comissão Reguladora;

III – Comissão Avaliadora;

IV – Comissão de Comunicação Institucional; e

V – investigadores e/ou grupos de investigadores.

CAPÍTULO V
DA COMUNICAÇÃO E DOS PRAZOS

Art. 7º Todos os formulários e documentos a serem remetidos ao Tribunal Superior Eleitoral para fins de pré-inscrição, inscrição, manifestação e recurso deverão ser:

a) encaminhados por SEDEX ou carta registrada endereçados à Secretaria de Tecnologia da Informação do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF, CEP 70070-600); ou

b) protocolizados no Protocolo Administrativo, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF); ou

c) encaminhados para o *e-mail* tps2016@tse.jus.br;

§ 1º Por não dispor de comprovação de recebimento e leitura, a comunicação por intermédio de *e-mail* é meramente alternativa e tem o objetivo de facilitar a comunicação dos investigadores ou grupo de investigadores.

§ 2º O Tribunal confirmará o recebimento de *e-mail* imediatamente após proceder à leitura da mensagem.

§ 3º No caso de o investigador ou o grupo de investigadores não receber a confirmação de leitura pelo TSE, no prazo por ele julgado conveniente, deverá encaminhar o conteúdo da mensagem e/ou material anexo por SEDEX ou protocolizá-lo no Tribunal, respeitando-se os prazos estabelecidos neste edital.

Art. 8º O sítio oficial do TPS será tps2016.tse.jus.br.

§ 1º As informações relacionadas ao evento serão publicadas no sítio oficial do TPS.

§ 2º Mensagens eletrônicas recebidas de investigadores ou grupo de investigadores serão respondidas por *e-mail*, exceto quando a resposta for de interesse geral, quando poderá ser publicada no sítio oficial do TPS.

Art. 9º As datas e prazos que norteiam o TPS estão informados no Calendário do Evento, anexo a este edital.

§ 1º Os prazos poderão ser prorrogados a critério do TSE.

§ 2º Quaisquer alterações de datas serão informadas no sítio oficial do TPS.

CAPÍTULO VI
DA PARTICIPAÇÃO

Art. 10. O TPS terá no máximo 25 pessoas participantes, observando-se o seguinte:

I – a participação poderá ser individual (investigador) ou em grupo de investigadores;

II – cada grupo de investigadores poderá ter de 2 a 5 membros;

III – Um participante não pode possuir mais de uma inscrição, seja em grupo ou individual.

IV – o total de grupos de investigadores somado ao de investigadores individuais não poderá ser superior a 10, ou seja, serão aceitas até 10 inscrições.

Parágrafo único. É vedada a participação, na condição de investigador e/ou de grupo de investigadores, de componentes das comissões definidas no art. 6º da Resolução 23.444/2015.

Art. 11. A participação, na condição de investigador e/ou de grupo de investigadores, está condicionada à seleção prévia, que será realizada em 3 etapas:

I – aprovação da pré-inscrição;

II – aprovação da inscrição; e

III – disponibilidade orçamentária e sorteio público.

Parágrafo único. A Comissão Avaliadora poderá, a seu critério, selecionar os planos de testes de até 2 (dois) investigadores ou grupos de investigadores que não foram sorteados.

CAPÍTULO VII
DA PRÉ-INSCRIÇÃO

Art. 12. A pré-inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Pré-Inscrição, que poderá ser obtido no sítio oficial do TPS.

Art. 13. O formulário Pré-Inscrição preenchido e os documentos comprobatórios exigidos deverão ser encaminhados, postados ou protocolizados no TSE, respeitados os prazos estabelecidos no Marco 1 do Calendário do Evento.

Art. 14. Terão sua pré-inscrição aprovada, na condição de investigador ou de grupo de investigadores, os cidadãos brasileiros maiores de 18 anos que preencham os requisitos constantes do formulário de pré-inscrição.

§ 1º Cada grupo de investigadores deverá designar um de seus componentes para representá-lo.

§ 2º Das pré-inscrições deverão constar os dados referentes a todos os componentes do grupo.

§ 3º Caso um dos membros do grupo de investigadores não atenda aos requisitos do formulário de pré-inscrição, o grupo não terá sua pré-inscrição aprovada.

§ 4º Os investigadores ou grupos de investigadores deverão informar, no momento do preenchimento do formulário de pré-inscrição, se desejam fazer o uso de recursos financeiros do TSE para o custeio de diárias e passagens.

§ 5º Pessoa jurídica poderá se pré-inscrever.

a) terá sua pré-inscrição aprovada a pessoa jurídica cujo investigador e/ou grupo de investigadores que a representará no TPS cumpra todas as exigências do edital.

b) não serão aceitas pré-inscrições de empresas sem registro no Cadastro Nacional de Pessoa Jurídica (CNPJ).

Art. 15. Na data estabelecida no Marco 2 do Calendário do Evento serão publicadas as pré-inscrições aprovadas no sítio oficial do TPS.

§ 1º O investigador ou grupo de investigadores que não tiver sua pré-inscrição aprovada poderá apresentar recurso ao Tribunal.

§ 2º O recurso deverá ser encaminhado, postado ou protocolizado no TSE, respeitado o prazo estabelecido no Marco 3 do Calendário do Evento.

§ 3º O resultado do recurso será apresentado no sítio oficial do TPS na data prevista no Marco 4 do Calendário do Evento.

Art. 16. Aos investigadores e/ou grupos de investigadores com a pré-inscrição aprovada e que tenham interesse, no dia e horário estabelecido no Marco 5 do Calendário do Evento, na Sede do TSE, será ministrada palestra referente ao funcionamento tecnológico do sistema eletrônico de votação.

§ 1° A palestra de que trata o *caput* deste artigo será transmitida pelo sítio do evento do TPS.

§ 2° Além dos investigadores e/ou grupos de investigadores com a pré-inscrição aprovada, poderão participar da palestra os componentes das comissões e demais interessados, devidamente autorizados pela Comissão Reguladora.

Art. 17. Os investigadores e/ou grupos de investigadores com a pré-inscrição aprovada, no dia da palestra, poderão agendar, respeitado o prazo estabelecido no Marco 6 do Calendário do Evento, visita à Sede do TSE para inspeção dos códigos-fonte.

§ 1º Os investigadores terão acesso ao código por meio de ferramenta de visualização fornecida pelo TSE.

§ 2º Só terão acesso aos códigos-fonte os investigadores e/ou grupos de investigadores que assinarem o termo de confidencialidade.

§ 3º Deverão assinar o termo de confidencialidade todos os investigadores que ingressarem no ambiente de apresentação dos códigos-fonte, mesmo que sejam membros de grupo.

§ 4º A assinatura do termo de confidencialidade dar-se-á no momento de ingresso do investigador no ambiente de apresentação dos códigos-fonte.

§ 5º Serão publicados no sítio oficial do TPS:

I – O modelo do termo de confidencialidade para fins de conhecimento prévio dos investigadores e/ou grupos de investigadores; e

II – O período reservado para a inspeção dos códigos-fonte.

§ 6º O tempo destinado aos investigadores e/ou grupo(s) de investigadores para inspeção dos códigos-fonte será estabelecido pelo TSE conforme a capacidade do ambiente e a quantidade de investigadores que manifestarem interesse.

§ 7º Não haverá custeio pelo Tribunal de diárias e passagens para essa fase do evento.

CAPÍTULO VIII
DA INSCRIÇÃO

Art. 18. A inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Plano de Teste, que poderá ser obtido no sítio oficial do TPS.

§ 1° Poderão apresentar plano de teste todos os investigadores e/ou grupos de investigadores com pré-inscrição aprovada.

§ 2° Cada investigador e/ou grupo de investigadores poderá apresentar mais de um plano de teste.

Art. 19. O formulário Plano de Teste preenchido e os documentos complementares, caso haja, deverão ser encaminhados, postados ou protocolizados no TSE, respeitado o prazo estabelecido no Marco 7 do Calendário do Evento.

Art. 20. Terão sua inscrição aprovada, na condição de investigador e/ou de grupo de investigadores, aqueles que tiverem seu plano de teste aprovado pela Comissão Reguladora.

Parágrafo único. não serão aprovados os planos de testes que:

I – não atenderem aos objetivos específicos de alterar a destinação dos votos ou fragilizar o sigilo do voto;

II – não atenderem ao objeto estabelecido no art. 2º deste edital;

III – não demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou

IV – forem entregues após o prazo estipulado no Marco 7 do Calendário do Evento.

Art. 21. Na data estabelecida no Marco 8 do Calendário do Evento, serão publicadas as inscrições aprovadas no sítio oficial do TPS.

§ 1º Os investigadores e/ou grupos de investigadores que não tiveram sua inscrição aprovada poderão apresentar recurso ao Tribunal, respeitado o prazo estabelecido no Marco 9 do Calendário do Evento.

§ 2º O resultado do recurso será apresentado no sítio oficial do TPS na data prevista no Marco 10 do Calendário do Evento.

Art. 22. A aprovação da inscrição do investigador e/ou do grupo de investigadores não garante a participação nos testes públicos de segurança.

CAPÍTULO IX
DA DISPONIBILIDADE ORÇAMENTÁRIA E DO SORTEIO PÚBLICO

Art. 23. Caso a quantidade de investigadores e/ou grupos de investigadores com inscrição aprovada seja superior à quantidade estipulada no art. 10 deste edital, far-se-á necessário realizar uma seleção entre as inscrições aprovadas. A seleção será realizada na seguinte sequência:

I – serão selecionados os investigadores individuais que não necessitem de recursos financeiros do TSE para o custeio de diárias e passagens;

a) caso a quantidade de investigadores individuais selecionados seja superior a 10, será realizado sorteio público entre esses e recusadas todas as demais inscrições aprovadas.

II – após a seleção dos investigadores individuais, caso haja disponibilidade de vagas, serão selecionados os grupos de investigadores que não necessitem de recursos financeiros do TSE para o custeio de diárias e passagens;

a) havendo grupos de investigadores que não necessitem do custeio de diárias e passagens em quantidade superior à quantidade de vagas, realizar-se-á sorteio entre os grupos respeitando-se os limites estabelecidos neste edital; e

b) caso todas as vagas tenham sido preenchidas, serão recusadas todas as demais inscrições aprovadas.

III – havendo disponibilidade de vagas:

a) será verificada a disponibilidade orçamentária do TSE para o custeio de diárias e passagens;

b) será realizado um orçamento do custo de diárias e passagens por investigador individual ou grupo de investigadores;

c) serão priorizados os investigadores ou grupos de investigadores com menor custo de diárias e passagens até o limite de vagas.

Art. 24. O sorteio público será realizado nas instalações do TSE, em data estabelecida no Marco 11 do Calendário do Evento.

Art. 25. Na data estabelecida no Marco 12 do Calendário do Evento, será publicado o resultado das inscrições selecionadas no sítio oficial do TPS.

§ 1º O investigador e/ou grupo de investigadores que não teve sua inscrição selecionada poderá apresentar recurso ao Tribunal, respeitado o prazo estabelecido no Marco 13 do Calendário do Evento.

§ 2º O resultado do recurso será apresentado no sítio oficial do TPS, na data estabelecida no Marco 14 do Calendário do Evento.

CAPÍTULO X
DAS INSCRIÇÕES SELECIONADAS

Art. 26. Os investigadores ou grupos de investigadores que optaram pelo custeio de deslocamento pelo TSE e que tiveram sua inscrição selecionada deverão requerer passagens e diárias ao Tribunal Superior Eleitoral.

§ 1º As passagens e diárias devem ser requeridas até a data estabelecida no Marco 15 do Calendário do Evento, utilizando-se do formulário Solicitação de Diárias e Passagens, disponível no sítio oficial do TPS.

§ 2º As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral.

§ 3º O custeio de diárias compreenderá o período equivalente às fases de inspeção dos códigos-fonte, de preparação e de realização do TPS, conforme estabelecido nos marcos 16, 17 e 18 do Calendário do Evento.

§ 4º Será aferida a presença por meio de lista de presença a ser assinada pelos participantes durante o evento.

§ 5º O Tribunal deverá requerer o reembolso do investigador ou membro do grupo de investigadores que:

I – tiver passagens e/ou diárias custeadas pelo Tribunal e não comparecer ao evento;

II – receber uma quantidade de diárias maior do que o período de comparecimento ao evento; e

III – outros casos em que a Comissão Reguladora entender que o Plano de Teste não foi executado conforme definido e por responsabilidade exclusiva do investigador ou grupo de investigadores.

Art. 27. Os investigadores ou grupos de investigadores selecionados declaram ter ciência de que:

I – devem disponibilizar à Comissão Reguladora toda a documentação sobre os materiais utilizados e seus procedimentos durante as atividades, independentemente do resultado obtido no TPS;

II – devem apresentar à Comissão Reguladora todos os materiais utilizados e seus procedimentos durante as atividades; e

III – autorizam o uso de sua imagem pela Justiça Eleitoral, com a finalidade de divulgar o processo do Teste Público de Segurança realizado pelo TSE, entendendo-se como imagem qualquer forma de representação, inclusive a fotográfica, bem como o processo audiovisual que resulta da fixação de imagens, com ou sem som, que tenha a finalidade de criar, por meio de sua reprodução, a impressão de movimento, independentemente dos processos de sua captação, do suporte usado inicial ou posteriormente para fixá-lo e dos meios utilizados para sua veiculação.

Art. 28. Os investigadores e/ou grupos de investigadores com a inscrição selecionada, e que tenham interesse, na data estabelecida no Marco 16 do Calendário do Evento, de 9 a 18 horas, na Sede do TSE, poderão inspecionar os códigos-fonte do sistema de eletrônico de votação.

§ 1º Só terão acesso aos códigos-fonte os investigadores e/ou grupos de investigadores que assinarem termo de confidencialidade.

a) deverão assinar o termo de confidencialidade todos os investigadores que ingressarem no ambiente de inspeção dos códigos-fonte, mesmo que sejam membros de grupo.

b) estarão dispensados de assinar o termo de confidencialidade os investigadores ou grupo de investigadores que já o tenham feito na fase de pré-inscrição.

c) a assinatura do termo de confidencialidade dar-se-á no momento de ingresso do investigador no ambiente de apresentação dos códigos-fonte.

CAPÍTULO XI
DA FASE DE PREPARAÇÃO

Art. 29. A fase de preparação consiste no período em que os investigadores e/ou grupos de investigadores poderão configurar os sistemas que serão utilizados no teste e elaborar seu plano de testes.

Art. 30. A fase de preparação realizar-se-á em período estabelecido no Marco 17 do Calendário do Evento, de 9 a 18 horas, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília /DF).

Parágrafo único. O local destinado à fase de preparação será divulgado no sítio oficial do TPS.

Art. 31. O Tribunal Superior Eleitoral disponibilizará aos investigadores e/ou grupos de investigadores, no ambiente do Teste Público de Segurança, os seguintes materiais e equipamentos:

I – folhas de papel em branco;

II – canetas esferográficas;

III – mesas;

IV – cadeiras;

V – microcomputadores padrão IBM-PC com plataforma Windows 7 e/ou Ubuntu Linux 14.04 64 bits, que não poderão ser conectados à internet;

VI – impressoras;

VII – ferramentas manuais (alicate, chaves de fenda e Philips e multímetro digital);

VIII – urna eletrônica modelo 2013; e

IX – outros materiais e equipamentos necessários, a critério da Comissão Reguladora.

Parágrafo único. Será de responsabilidade dos investigadores e/ou grupos de investigadores a configuração dos equipamentos necessários à realização de seu plano de testes de segurança.

Art. 32. O microcomputador disponibilizado pelo TSE (artigo 31, V), a urna eletrônica (artigo 31, VIII) e os demais equipamentos, eventualmente preparados pelos investigadores e/ou grupos de investigadores participantes, serão lacrados ao término da fase de preparação.

§ 1° Os equipamentos referidos no *caput* deste artigo terão sua integridade verificada no dia do teste pelos investigadores e/ou grupo de investigadores e pelos componentes das comissões referidas no art. 6º deste edital.

§ 2° Eventual alteração no plano de testes, já entregue pelos investigadores e/ou grupos de investigadores e aprovado pela Comissão Reguladora, ficará sujeita à nova aceitação.

Art. 33. Durante a fase de preparação, será disponibilizado local para a visualização do código-fonte em um ambiente segregado ao da realização do Teste Público de Segurança, observando-se as seguintes condições:

I – é vedada a extração, impressão e/ou reprodução, mesmo que parcial, do código-fonte;

II – é vedado ingressar no ambiente segregado ao da realização dos testes com qualquer instrumento que permita a cópia do código-fonte.

III – são permitidas anotações que não confrontem o termo de confidencialidade.

a) as anotações estarão sujeitas à análise da Comissão Reguladora;

b) compete ao investigador se responsabilizar por suas anotações; e

c) as anotações serão de uso restrito ao ambiente do TPS.

Parágrafo único. As vedações referidas nos incisos I e II deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente segregado ao da realização do Teste Público de Segurança.

CAPÍTULO XII
DO TESTE PÚBLICO DE SEGURANÇA

Art. 34. O Teste Público de Segurança no sistema eletrônico de votação realizar-se-á em período estabelecido no Marco 18 do Calendário do Evento, de 9 a 18 horas, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília /DF).

§ 1° Findado o prazo estabelecido e verificada, excepcionalmente, a necessidade de continuidade de realização de algum Plano de Teste, devido a sua significativa contribuição para o alcance do objetivo do TPS, a Comissão Avaliadora poderá recomendar à Comissão Reguladora a extensão do prazo do TPS por mais 1 (um) dia.

I – A recomendação deverá ser feita por escrito e justificada.

II – A Comissão Reguladora decidirá a respeito da recomendação e, no caso de não acatá-la, deverá justificar a decisão.

III – Caso haja necessidade de alteração de passagens e/ou da quantidade de diárias, a Comissão Reguladora deverá verificar a existência de disponibilidade orçamentária para o custeio das alterações.

§ 2° O local destinado ao Teste Público de Segurança será divulgado no sítio oficial do TPS.

Art. 35. Somente serão executados os planos de testes dos investigadores e/ou grupos de investigadores que:

I – tiverem sua inscrição aprovada e selecionada.

II – estiverem presentes no momento da realização dos testes.

§ 1° Somente serão autorizados os planos de testes que forem aprovados e atendam aos requisitos deste edital, que não causem danos físicos aos equipamentos e às instalações disponibilizados para os citados testes e que forem tecnicamente viáveis.

§ 2° Para os fins do inciso II deste artigo, os grupos de investigadores poderão ser representados por apenas um de seus componentes, ressalvado os que receberam diárias e passagens custeadas pela Justiça Eleitoral.

Art. 36. Ao final da fase de realização do Teste Público de Segurança, cada investigador ou grupo de investigadores deverá apresentar Relatório

Investigador das ações executadas e resultados alcançados, de acordo com as regras definidas neste edital.

Art. 37. Os investigadores e/ou grupos de investigadores, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, deverão apresentar as respectivas sugestões de melhoria.

§ 1º Em data estabelecida pelo TSE, anterior à Cerimônia Oficial de Assinatura Digital e Lacração dos Sistemas a serem utilizados nas Eleições de 2016, os investigadores e/ou grupos de investigadores poderão ser convocados a repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 2º A nova execução dos testes de que trata o parágrafo anterior não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.

§ 3º Para o disposto no § 1º, as modificações realizadas serão apresentadas de acordo com o cronograma a ser definido pela Comissão Reguladora.

§ 4º Os investigadores e/ou grupos de investigadores somente poderão se manifestar publicamente sobre a falha ou vulnerabilidade encontrada após a divulgação do relatório da Comissão Avaliadora.

CAPÍTULO XIII
DA AUDIÊNCIA PÚBLICA

Art. 38. Em data estabelecida no Marco 19 do Calendário do Evento, de 10 a 11 horas, na Sede do TSE, será realizada audiência pública com a finalidade de:

I – divulgar os resultados e as conclusões do Teste Público de Segurança; e

II - entregar certificado de participação aos investigadores e grupos de investigadores.

§ 1° Somente será concedido o certificado referido no inciso II deste artigo aos investigadores e grupos de investigadores que tiveram seus planos de testes devidamente executados, independentemente do resultado.

§ 2° Além do disposto no § 1º deste artigo, somente será concedido o certificado aos componentes dos grupos que estiveram presentes quando da realização do respectivo teste de segurança.

§ 3° O local da audiência pública será divulgado no sítio oficial do TPS.

CAPÍTULO XIV
DAS DISPOSIÇÕES GERAIS

Art. 39. As atividades executadas durante a fase de preparação e de realização do Teste Público de Segurança poderão ser registradas pelo TSE em áudio e vídeo.

Art. 40. Para ingresso no ambiente destinado à fase de preparação e à de realização do Teste Público de Segurança, deverá ser observado que:

I – o ingresso com CD-ROM ou DVD-ROM, já utilizado e desde que não regravável, será autorizado;

II – a entrada de outros equipamentos ou dispositivos além daqueles citados no inciso I deste artigo, desde que não tenham acesso à internet, deverá ser autorizada pela Comissão Reguladora;

III – os investigadores e/ou grupos de investigadores poderão utilizar os *softwares* que julgarem necessários e instalá-los no microcomputador disponibilizado pelo TSE, observando-se o disposto nos incisos I e II deste artigo;

IV – o ingresso com materiais impressos será permitido;

V – os equipamentos, dispositivos eletrônicos e materiais citados nos incisos I, II e III, quando aprovados, poderão ficar retidos no Tribunal Superior Eleitoral por até 60 dias após o encerramento da realização do Teste Público de Segurança.

§ 1° Os equipamentos ou dispositivos que tenham ficado retidos no TSE estarão à disposição dos participantes após o prazo citado no inciso V deste artigo.

§ 2° As vedações referidas nos incisos I a V deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente destinado à fase de preparação e à fase de realização do Teste Público de Segurança.

Art. 41. O ingresso no ambiente do Teste Público de Segurança e no ambiente segregado será restrito:

I – aos investigadores e/ou grupos de investigadores;

II – aos integrantes das comissões referidas no art. 6º deste edital;

III – às demais pessoas autorizadas pela Comissão Reguladora.

Art. 42. Haverá, no ambiente de testes, computadores conectados a internet para eventuais consultas pelos investigadores e/ou grupos de investigadores, sob supervisão da Comissão Reguladora.

Art. 43. A Comissão Avaliadora somente poderá ter acesso ao código-fonte em caso de necessidade inafastável, sendo o acesso autorizado pela Comissão Reguladora, mediante a assinatura de termo de confidencialidade.

Art. 44. O relatório a ser apresentado pela Comissão Avaliadora deve observar as regras de edição e publicação definidas pela Comissão Organizadora.

Art. 45. Este edital será publicado no DJe/TSE e divulgado no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 46. Será dada publicidade à composição das comissões referidas no art. 6º deste edital por meio do DJe/TSE e divulgação no sítio oficial do TPS.

Art. 47. Integra este edital o cronograma do Teste Público de Segurança, anexo.

Art. 48. Os casos omissos serão dirimidos pelo Ministro Coordenador do Teste Público de Segurança.

Brasília, 30 de novembro de 2015.

ANEXO – CALENDÁRIO DO EVENTO

Marco	Referência	Descrição do marco	Prazo/período
Marco 1	Art. 13	Encaminhamento do formulário de Pré-Inscrição preenchido e dos documentos comprobatórios exigidos.	1º a 09/12/2015
Marco 2	Art. 15	Publicação das pré-inscrições aprovadas.	11/12/2015
Marco 3	§ 2º do Art. 15	Apresentação de recurso referente à fase de pré-inscrição.	11 a 15/12/2015
Marco 4	§ 3º do Art. 15	Publicação do resultado do recurso referente à fase de pré-inscrição.	18/12/2015
Marco 5	Art. 16	Palestra referente ao funcionamento tecnológico do sistema eletrônico de votação	11/01/2016
Marco 6	Art. 17	Inspeção dos códigos-fonte.	11 a 13/01/2016
Marco 7	Art. 19	Encaminhamento do formulário Plano de Teste preenchido e os documentos complementares, caso haja.	11 a 22/01/2016
Marco 8	Art. 21	Publicação das inscrições aprovadas.	1º/02/2016
Marco 9	§ 1º do Art. 21	Apresentação de recursos referente à fase de inscrição aprovada.	1º a 03/02/2016
Marco 10	§ 2º do Art. 21	Publicação do resultado do recurso referente à fase de inscrição aprovada.	05/02/2016
Marco 11	Art. 24	Sorteio público para seleção de inscrições.	15/02/2016
Marco 12	Art. 25	Publicação do resultado das inscrições selecionadas.	15/02/2016
Marco 13	§ 1º do Art. 25	Apresentação de recursos referente à fase de inscrição selecionada.	15 a 17/02/2016
Marco 14	§ 2º do Art. 25	Publicação do resultado do recurso referente à fase de inscrição selecionada.	19/2/2016
Marco 15	§ 1º do Art. 26	Requisição de passagens e diárias.	19 a 24/2/2016
Marco 16	Art. 28	Inspeção dos códigos-fonte.	7/03/2016
Marco 17	Art. 30	Preparação do ambiente dos testes.	7/03/2016
Marco 18	Art. 34	Realização dos Testes Públicos de Segurança.	8 a 10/03/2016 11/03*
Marco 19	Art. 38	Audiência pública para divulgação dos resultados, conclusões do Teste Público de Segurança e entrega do certificado de participação.	15/03/2016

* dia adicional, conforme estabelecido no § 1º do Art. 34.

Anexo B – Portarias de designação das comissões

Portaria-TSE n° 471/2015

Publicado no Diário da Justiça Eletrônico 183
05.10.15 Pág. 02/03

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 471, de 01 de outubro de 2015

Institui Comissões para atuar na realização do Teste Público de Segurança - TPS.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto nos arts. 8º, 9º e 11 da Resolução - TSE nº 23.444,de 30 de abril de 2015.

RESOLVE:

Art. 1º Ficam criadas na forma do Anexo, as Comissões Organizadora, Reguladora e de Comunicação Institucional, para atuar na realização do Teste Público de Segurança - TPS, de que trata a Resolução TSE nº 23.444, de 30 de abril de 2015.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **José Antônio Dias Toffoli**, **Presidente**, em 01/10/2015, às 18:02, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0017880** e o código CRC **5264EBF6**.

Sei 1751-2

ANEXO

TESTE PÚBLICO DE SEGURANÇA

COMISSÃO ORGANIZADORA (ART. 8º)	
Assessoria de Gestão Estratégica	Fabiano de Andrade Lima
Administração	Eliane Josimar Alves
Segurança	Hélio Ferreira de Faria
Infraestrutura de TI	Luciano Teixeira Andrade
Cerimonial	Paula Cristiane Amorim de Souza
Imprensa e Comunicação Social	Jean Fábio Peverari

COMISSÃO REGULADORA (ART. 9º)	
Integrante com conhecimentos jurídicos, indicado pela Presidência do Tribunal	Ana Lúcia Andrade de Aguiar
Integrante de TI	José de Melo Cruz (CSELE/STI)
Integrante de TI	Rafael Fernandes de Barros Costa Azevedo (CLOGI/STI)
Integrante de TI	Cristiano Moreira Andrade (COINF/STI)
Integrante de TI	Elmano Amâncio de Sá Alves (ASPLAN/STI)
Integrante de TI	Rodrigo Carneiro Munhoz Coimbra (SEVIN/CSELE/STI)
Integrante de TI	Júlio Valente da Costa Júnior (SEPEL/CSELE/STI)
Integrante de TI	Célio Castro Wermelinger (SESPE/CSELE/STI)
Integrante de TI	Marcelo Carneiro Rodrigues (SESOP/COINF/STI)
Integrante de TI	Ivanildo Ferreira Gomes (SEREDE/COINF/STI)
Integrante de TI	Lucas Ferreira Lima (EP/ASPLAN/STI)
Integrante de TI	Antônio Ésio Marcondes Salgado (INPE)
Imprensa e Comunicação Social	Juliana Mendes Gonzaga Neiva

COMISSÃO DE COMUNICAÇÃO INSTITUCIONAL (ART. 11)	
Imprensa e Comunicação Social	Juliana Mendes Gonzaga Neiva
Imprensa e Comunicação Social	Márcio Meireles (Coord. Com. Institucional)
Integrante de TI	Giuseppe Dutra Janino
Assessoria de Gestão Estratégica	Fabiano de Andrade Lima

Portaria-TSE n° 553/2015

Ano 2015, Número 216 Brasília, segunda-feira, 16 de novembro de 2015 Página 2

Atos da Presidência

Portarias

Comissão Avaliadora. Teste Público de Segurança - TPS

Portaria TSE nº 553, de 12 de novembro de 2015.

Institui Comissão para atuar na realização do Teste Público de Segurança - TPS.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 10 da Resolução - TSE nº 23.444,de 30 de abril de 2015.

RESOLVE:

Art. 1º Fica criada a Comissão Avaliadora, para atuar na realização do Teste Público de Segurança - TPS, de que trata a Resolução TSE n° 23.444, de 30 de abril de 2015, com a seguinte composição:

I - representante indicado pelo Ministro Presidente, Juíza Ana Lúcia de Andrade de Aguiar;

II - membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação: Prof. Dr. Mamede Lima Marques; Dr. Osvaldo Catsumi Imamura; Prof. Dr. Jamil Salem Barbar; Dr. Antônio Montes Filho;

III - representante do Ministério Público Federal, Dr. Ângelo Goulart Villela;

IV - representante da Ordem dos Advogados do BrasilDr. Erick Wilson Pereira;

V - representante do Congresso Nacional, Dr. Antonio de Souza Dantas;

VI - perito criminal federal da área de Informática, do Departamento de Polícia Federal, Dr. Thiago de Sá Cavalcanti;

VII - engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (CREA), indicado pelo Conselho Federal de Engenharia e Agronomia (CONFEA), Dr. Lúcio Antônio Ivar do Sul;

VIII - representante da Sociedade Brasileira de Computação (SBC), Professor Diego Aranha;

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Ministro DIAS TOFFOLI

Documento assinado eletronicamente por **JOSÉ ANTÔNIO DIAS TOFFOLI, PRESIDENTE**, em 12/11/2015, às 19:40, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0033419&crc=06183393, informando, caso não preenchido, o código verificador **0033419** e o código CRC **06183393**.

SECRETARIA JUDICIÁRIA

Coordenadoria de Processamento - Seção de Processamento I

Decisão monocrática

PUBLICAÇÃO Nº 229/2015/SEPROC1

RECLAMAÇÃO Nº 512-52.2015.6.00.0000 PORTO ALEGRE-RS

RECLAMANTE: CÁSSIO DE JESUS TROGILDO

ADVOGADOS: GUSTAVO HENRIQUE CAPUTO BASTOS E OUTROS

Portaria-TSE n° 202/2016

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 202, de 3 de março de 2016.

Altera composição da Comissão Reguladora do Teste Público de Segurança-TPS, de que trata a Portaria TSE nº 471, de 1º de outubro de 2015.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto nos arts. 8º, 9º e 11 da Resolução - TSE nº 23.444, de 30 de abril de 2015,

R E S O L V E:

Art. 1º Alterar o Anexo da Portaria TSE nº 471, de 1º de outubro de 2015, que institui comissões para atuar na realização do Teste Público de Segurança - TPS, na parte relativa à Comissão Reguladora, para incluir o servidor CRISTIANO PEÇANHA CORREA, em substituição ao servidor LUCAS FERREIRA LIMA.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Ministro DIAS TOFFOLI

Presidente

Documento assinado eletronicamente por **JOSÉ ANTÔNIO DIAS TOFFOLI**, **PRESIDENTE**, em 03/03/2016, às 18:42, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0087392&crc=7669460C, informando, caso não preenchido, o código verificador **0087392** e o código CRC **7669460C**.

Anexo C – Resultado definitivo das inscrições

Nos termos do artigo 25 do Edital do Teste Público de Segurança, a Comissão Reguladora declara inscritos os seguintes participantes e seus respectivos planos de testes, listados abaixo:

GRUPO DE INVESTIGADORES

Grupo 1: Coordenado por André Henrique de Siqueira.
Inscrição: APROVADA.
Plano de teste: Teste do Sistema de Apuração por Votação Totalmente Eletrônica (digitar BU). Situação: APROVADO.
Ressalvas: O plano apresentado prevê o uso de *notebook* próprio. Não há óbice quanto à utilização do equipamento, entretanto sua utilização deverá ser autorizada pela comissão reguladora.

Grupo 2: Coordenado por Charles Figueredo de Barros
Inscrição: APROVADA.
Plano de teste: Ataque ao sigilo do voto. Situação: APROVADO.
Plano de teste: Análise da segurança do armazenamento de arquivos e valores na memória da urna e nas mídias removíveis. Situação: NÃO APROVADO.
Motivo: O plano apresenta a análise dos arquivos das mídias da urna como um fim em si mesmo, sem utilizá-la como instrumento para exploração de uma vulnerabilidade. Dessa forma, o plano de testes apresentado está em desconformidade com o objetivo do Edital do Teste Público de Segurança, o qual preconiza, em seu artigo 3º, parágrafo único: "O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição e apresentar as respectivas sugestões de melhoria".
Plano de teste: Análise de práticas de programação relacionadas ao uso de primitivas criptográficas e outros aspectos de segurança do código-fonte. Situação: NÃO APROVADO.
Motivo: O plano apresenta a análise de código como um fim em si mesmo, sem utilizá-la como instrumento para exploração de uma vulnerabilidade. Dessa forma, o plano de testes apresentado está em desconformidade com o objetivo do Edital do Teste Público de Segurança, o qual preconiza, em seu artigo 3º, parágrafo único: "O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição e apresentar as respectivas sugestões de melhoria".

Grupo 3: Coordenado por Dawilmar Guimarães de Araújo
Inscrição: NÃO APROVADA.
Motivo: O grupo não apresentou o plano de teste.

Grupo 4: Coordenado por Elisabete Ewaldt
Inscrição: APROVADA.
Plano de teste: Tentativa de fraude na destinação dos votos na urna através de controle dos dispositivos de teclado e impressora. Situação: APROVADO.
Ressalva: O plano apresentado prevê o uso de *notebook* próprio conectado à internet. Não há óbice quanto ao uso de equipamento próprio, entretanto a utilização deverá ser autorizada pela comissão reguladora, e não poderá haver conexão com a internet, conforme artigo 40, inciso II, do Edital do Teste Público de Segurança. Estarão disponíveis aos investigadores computadores com acesso à internet. Será permitida a utilização, no

ambiente de execução dos testes, de material obtido durante o acesso à internet.

Grupo 5: Coordenado por Luis Fernando de Almeida
Inscrição: APROVADA.
Plano de Teste: Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual. Situação: APROVADO.

INVESTIGADORES INDIVIDUAIS

João Felipe
Inscrição: APROVADA.
Planos de testes: *Reflash* de urna, Registrador do teclado, Destruidor de votos e Root Kit JE Connect. Situação: APROVADO.

Marcelo Muzili
Inscrição: NÃO APROVADA.
Plano de teste: Invasão no transporte dos dados no sistema de votação. Situação: NÃO APROVADO.
Motivo: O plano de teste apresentado solicita acesso ao ambiente de totalização, às máquinas servidoras e ao banco de dados, em desconformidade com o artigo 20, parágrafo único, inciso II, o qual determina que o plano de teste deve atender ao objeto estabelecido no artigo 2º do Edital do Teste Público de Segurança. O artigo 2º, § 2º, explicita o que não é objeto do teste público de segurança: "Não serão objeto do TPS os seguintes elementos dos sistemas e de seus ambientes: .... IV – totalização (TOT) e gerenciamento da totalização (GER); V – acesso às máquinas servidoras; VI – acesso aos bancos de dados".

Luís Felipe Féres Santos
Inscrição: NÃO APROVADA.
Motivo: O investigador não apresentou o plano de teste.

Raimundo Borges da Mota Júnior
Inscrição: NÃO APROVADA.
Motivo: O investigador não apresentou o plano de teste.

Wagner Rafael da Silva Peixoto
Inscrição: NÃO APROVADA.
Motivo: O investigador não apresentou o plano de teste.

Walter Gabriel Kentenich Silva
Inscrição: NÃO APROVADA.
Motivo: O investigador não apresentou o plano de teste.

Anexo D – Planos de teste do sistema eletrônico de votação

Grupo 1

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste Teste do Sistema de Apuração Por Votação Totalmente Eletrônica (digitar BU)		
Instituição proponente (se aplicável) Universidade de Brasília (UnB)		
Responsável	Nome: Sérgio Freitas da Silva *E-mail*: sergio.freitas.silva@gmail.com Telefone (do autor ou responsável): (61) 8170-8727	
Resumo do teste (máximo 120 caracteres)	O teste proposto refere-se ao Sistema de Apuração (SA), especificamente à funcionalidade identificada como "Votação totalmente eletrônica (digitar BU)" que permite a apuração através da digitação de um Boletim de Urna. Essa operação ocorre como medida de contingência, por exemplo, nos casos de falhas nas urnas em que não tenha sido possível a recuperação dos dados.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) (X) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit JE Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** (X) Urna eletrônica ( ) Mídias ( ) *Kit JE Connect* ***Procedimentos*** ( ) Geração de mídias ( ) Carga da urna (X) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	300 minutos	
Extensão do ataque	(X) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimentos do Sistema de Apuração, regras de geração do Boletim de Urna e Código Verificador.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O teste proposto refere-se ao Sistema de Apuração (SA), especificamente à funcionalidade identificada como "Votação totalmente eletrônica (digitar BU)" que permite a apuração através da digitação de um Boletim de Urna. Essa operação ocorre como medida de contingência, por exemplo, nos casos de falhas nas urnas em que não tenha sido possível a recuperação dos dados.

Conforme descrito na Figura 1, o procedimento do teste consiste na geração de um Boletim de Urna falso com alteração da quantidade e/ou destinação dos votos (item 1, da Figura 1). Esse Boletim de Urna falso é digitado (item 2) e validado (item 3) pelo Sistema de Apuração (SA) que homologa (item 4) esses dados falsos e gera os documentos e arquivos que serão enviados (item 5) para a apuração geral dos votos.

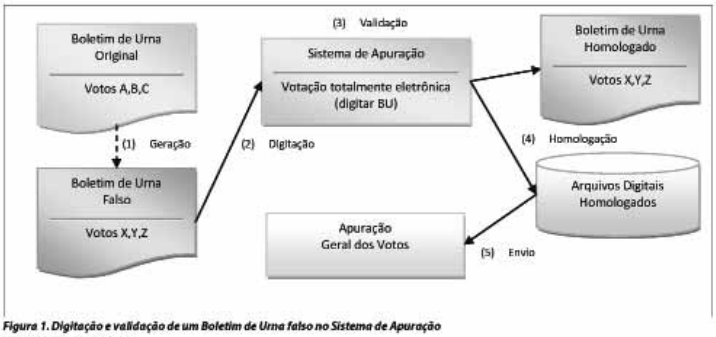


Figura 1. Digitação e validação de um Boletim de Urna falso no Sistema de Apuração
Fonte: Elaboração própria.

2.2 – Fundamentação teórica

A Constituição Federal define que "a soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos, nos termos da lei" (Art. 14, caput, da Constituição Federal de 1988). O valor igual para todos refere-se ao princípio do sufrágio igual, ou do voto igual, que reconhece a cada eleitor um único voto (*one man, one vote*), pois cada cidadão deve ter o mesmo peso político e a mesma influência, ou seja, a nenhum eleitor será atribuído mais voto do que a outros (Da Silva, 1992). Diz-se igual o valor quando o voto de cada eleitor tem o mesmo peso, independentemente de sua posição, fortuna, religião, clã social ou outra forma de discriminação (Queiroz, 1998).

Ocorre que durante o processo de votação podem ocorrer diversos tipos de problemas, incluindo falhas no *hardware*, *software* e procedimentos operacionais executados pelos participantes. Nesses casos, para cumprir os requisitos legais, incluindo os referidos princípios constitucionais, a Justiça Eleitoral prevê a adoção de procedimentos de contingência que visam sanar esses problemas, por exemplo, garantindo a continuidade da votação e a recuperação dos votos em caso de falhas.

Um desses procedimentos de contingência utilizados na apuração é oferecido pelo Sistema de Apuração (SA), também conhecido como Sistema de Voto Cantado (SVC). O SVC é um sistema de apuração eletrônica, executado através do microterminal, que proporciona maior agilidade ao processo de apuração de votos por cédulas, quando houver (Brasil, 2016a). Segundo Portelinha (2012), o conjunto normalizador da apuração por esse sistema é formado pelas regras vindas com a Resolução TSE n. 20.292, de 6 de agosto de 1998 - somadas às da Resolução TSE n. 20.103, de 3 de março de 1998, às da Lei n. 9.504, de 30 de setembro de 1997, e o Código eleitoral.

Nesse contexto, propõe-se o teste do Sistema de Apuração (SA), especificamente a funcionalidade identificada como "Votação totalmente eletrônica (digitar BU)" que permite a apuração através da digitação de um Boletim de Urna existente. Essa operação ocorre como medida de

contingência, por exemplo, nos casos de falhas nas urnas em que não tenha sido possível a recuperação dos dados. Essa funcionalidade está disponível na opção [4] do menu "Apurar seção", conforme descrito na Figura 2.

Figura 2 – Sistema de Apuração
Fonte: Elaboração própria (foto da urna realizada durante a inspeção dos códigos).

Ao escolher a opção "[4] - Votação totalmente eletrônica (digitar BU)", o Sistema de Apuração permite a digitação dos dados de um Boletim de Urna, incluindo o "Código Verificador" presente em cada seção do boletim. O código verificador é um resumo (*hash*) do conteúdo do Boletim de Urna, constituído por cinco dígitos (10^5 possibilidades) e, segundo relatado por técnicos do Tribunal Superior Eleitoral, funciona somente como um mecanismo de controle de erros de digitação. De fato, da forma como se encontra programado atualmente, esse código verifica somente a integridade do conteúdo impresso no boletim, sem qualquer controle de autenticidade do documento. O processo de digitação do Código Verificador no Sistema de Apuração é descrito na Figura 3.

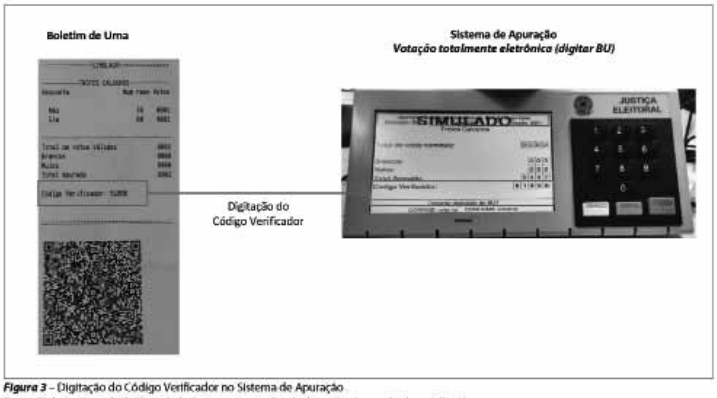


Figura 3 – Digitação do Código Verificador no Sistema de Apuração
Fonte: Elaboração própria (foto do boletim e urna realizada durante a inspeção dos códigos).

Uma vulnerabilidade existente no atual sistema eletrônico de votação é a ausência de um mecanismo automatizado de autenticação dos documentos impressos pela urna eletrônica, em especial o Boletim de Urna. Essa vulnerabilidade permite que um inimigo conhecendo, ou

deduzindo, as regras de verificação de integridade (Código Verificador) possa gerar Boletins de Urna falsos e comprometer a segurança do processo eleitoral.

Para eliminar essa vulnerabilidade pode-se utilizar a assinatura digital para que o Tribunal Superior Eleitoral (TSE) assine digitalmente os documentos impressos na urna, incluindo o Boletim de Urna, permitindo aos interessados conferir a autenticidade dos documentos a partir de um código de autenticação impresso no documento (assinatura digital). Segundo Carvalho (2000), a assinatura digital deve possuir os mesmo requisitos de uma assinatura tradicional. As assinaturas digitais podem utilizar esquemas baseados nos algoritmos de chave pública: a chave particular é utilizada pelo assinante (TSE) e a chave pública é utilizada para verificar a autenticidade da assinatura. Dessa forma, a assinatura digital auxilia nos seguintes atributos da segurança da informação: autenticidade, integridade e não repúdio.

Um exemplo de verificação de autenticidade é o serviço de emissão de Certidão de quitação eleitoral, oferecido pelo próprio Tribunal Superior Eleitoral (Brasil, 2016b). Nesse serviço é fornecido um código (de 16 caracteres) que pode ser digitado pelo interessado para verificar a autenticidade da Certidão de quitação eleitoral emitida pelo órgão. Outro mecanismo de autenticação bastante crítico é utilizado no sistema de loterias da Caixa Econômica Federal, nesse caso o recibo da aposta possui um código de autenticação para evitar fraudes, conforme destacado na Figura 4.

Figura 4 – Recibo de aposta da Mega-Sena com código de autenticação
Fonte: Elaboração própria (volante particular digitalizado).

Referências

Brasil (1997). Lei n. 9.504, de 30 de setembro de 1997.
Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9504.htm

Brasil (1998). Resolução TSE n. 20.292, de 6 de agosto de 1998 e Resolução TSE n. 20.103, de 3 de março de 1998.

Brasil (2016a). Página do Tribunal Regional Eleitoral do Distrito Federal. Conceitos úteis.
Disponível em: http://www.tre-df.jus.br/institucional/ouvidoria/conceitos-uteis

Brasil (2016b). Certidão de quitação eleitoral.
Disponível em: http://www.tse.jus.br/eleitor/servicos/certidoes/certidao-de-quitacao-eleitoral

Carvalho, Daniel Balparda de (2000). Segurança de dados com criptografia: métodos e algoritmos. Rio de Janeiro: Book Express.

Da Silva, José Afonso (1992). Curso de direito constitucional positivo. Malheiros Ed.

Queiroz, Arl Ferreira de (1998). Direito eleitoral. 4. ed. Goiânia: Jurídica IEPC. p. 44.

Portelinha, Luiz Henrique Martins (2012). Apuração eleitoral pelo sistema "Voto Cantado".
Disponível em: https://www.tre-sc.jus.br/site/resenha-eleitoral/edicoes-impressas/integra/2012/06/apuracao-eleitoral-pelo-sistema-voto-cantado/index6ca2.html?no_cache=1&cHash=4e128f5842a5fc5ccdb29a2b5143ba17

2.3 – Precondições para o teste

O teste fundamenta-se na hipótese que um Boletim de Urna falso pode ser digitado e validado pelo Sistema de Apuração (SA) tornando-se legítimo após sua homologação pelo sistema.

Nesse sentido, o teste pressupõe que um Boletim de Urna falso possa ser digitado no Sistema de Apuração após o relaxamento dos seguintes mecanismos e procedimentos-padrão de segurança:

1. Disponibilização da bobina da impressora (contendo o papel térmico timbrado original);
2. Impressão de um Boletim de Urna falso no papel original (timbrado);
3. Troca do Boletim de Urna original pelo Boletim de Urna falso;
4. Invalidação da urna eletrônica e mídias de modo a inviabilizar o Sistema de Recuperação;

A lista dos recursos necessários para a realização do teste é a seguinte:

1. Recursos materiais
    1. Recursos do TSE:
        1. Urna eletrônica com o Sistema de Apuração instalado e disponível para teste;
    2. Recursos fornecidos pelos investigadores:
        1. Impressora térmica Diletech (58mm);
        2. Notebook (Core I7, 8GB RAM) com Windows 7 Ultimate;
        3. Visual Studio Express 2013 (com C++);
        4. Biblioteca OpenSSL (32 bits);
        5. Código-fonte do teste para geração e impressão do Boletim de Urna (em C++);
2. Recursos humanos
    1. Técnico do TSE: com conhecimentos na operação do Sistema de Apuração;
    2. Investigadores: analistas e desenvolvedores com conhecimentos dos procedimentos de testes;

2.4 – Escopo – Superfície de ataque

Os seguintes componentes do sistema de votação eletrônica sofrerão atuação/alteração durante o teste:

1. Material:
    1. Bobina da impressora;
2. Procedimentos:
    1. Impressão de um falso boletim de urna;
    2. Substituição do boletim de urna original pelo falso boletim de urna;

2.5 – Janela de atuação simulada do atacante

A atuação do atacante deverá ocorrer nos seguintes instantes:

1. Após a impressão do boletim de urna original;
    a. Na troca do boletim de urna original pelo boletim de urna falso;

2.6 – Pontos de intervenção

Os pontos de intervenção são os seguintes:

1. Software
    1. Sistema de Apuração;
2. Hardware
    1. Impressora;
3. Equipamentos e acessórios
    1. Bobina da impressora;
4. Procedimento
    1. Impressão do Boletim de Urna

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

2.7 – Passos a serem realizados e material necessário

Os materiais necessários à realização dos testes são os seguintes:

1. Sob responsabilidade do TSE
    1. Urna Eletrônica com o Sistema de Apuração ativo e funcional
2. Sob responsabilidade dos investigadores:
    1. Impressora térmica Oletech (58mm);
    2. Notebook (Core I7, 8GB RAM) com Windows 7 Ultimate;
    3. Visual Studio Express 2013 (com C++);
    4. Biblioteca OpenSSL (32 bits);
    5. Código-fonte do teste para geração e impressão do Boletim de Urna (em C++);

O teste pressupõe que um Boletim de Urna falso possa ser digitado no Sistema de Apuração após o relaxamento dos mecanismos e procedimentos-padrão de segurança citados anteriormente.

O procedimento do teste é composto pelas seguintes etapas:

1. Simular uma votação na urna eletrônica e gerar um Boletim de Urna original (tempo estimado: 60 minutos);
2. Levantar os dados da votação, incluindo informações do pleito e do processo eleitoral (tempo estimado: 30 minutos);
3. Gerar e imprimir boletins de urna falsos (tempo estimado: 180 minutos);
    a. Opcionalmente, pode-se apenas gerar os dados falsos do boletim de urna (sem necessidade de impressão);
4. Digitar o Boletim de Urna falso, ou os dados falsos gerados, e verificar se são validados pelo Sistema de Apuração (tempo estimado: 30 minutos);
5. Fim

2.8 – Possíveis resultados e impacto

Os resultados esperados são os seguintes:

1. Tipo do resultado esperado
    1. Alteração do destino e quantidade de votos;
2. Extensão do ataque
    1. Urna;

A probabilidade esperada de sucesso do ataque é de 100% (cem por cento), considerando que a etapa de digitação do Boletim de Urna falso no Sistema de Apuração não prevê autenticação do Boletim de Urna.

2.9 – Rastreabilidade

Considerando a inexistência de mecanismos de autenticação do Boletim de Urna, considera-se inviável a detecção do ataque durante a digitação do boletim no Sistema de Apuração.

Nesse caso, a detecção do ataque poderia ocorrer somente antes do Sistema de Apuração através dos procedimentos de fiscalização dos envolvidos no processo.

2.10 – Solução proposta

Para solucionar as vulnerabilidades identificadas recomenda-se a adoção das seguintes soluções:

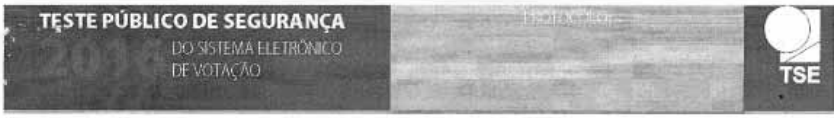
1. Refatorar a função de geração do código de verificação atual para torná-la mais robusta;
2. Disponibilizar um código de autenticação impresso no Boletim de Urna que permita verificar a integridade e a autenticidade do conteúdo impresso;
    a. Esse código de autenticação pode ser baseado em uma assinatura digital que possa ser verificada pelos cidadãos, fiscais e demais participantes do processo eleitoral;

Oportunamente, para eliminar eventuais vulnerabilidades, recomenda-se a adoção de mecanismos de autenticação em todos os documentos impressos na urna eletrônica, incluindo a Zerésima e o novo registro impresso do voto (art. 59-A da Lei 9.504).

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Grupo 2

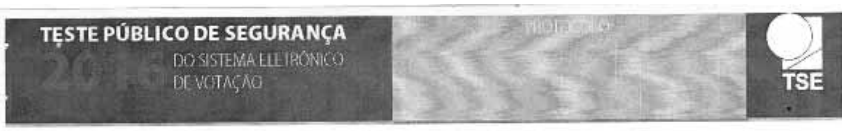


PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Título do plano de teste Ataque ao sigilo do voto		
Instituição proponente (se aplicável)		
Responsável	Nome: Charles Figueredo de Barros *E-mail*: charles.barros@ppgi.ufrj.br Telefone (do autor ou responsável): (21) 99288-3429	
Resumo do teste (máximo 120 caracteres)	Tentativa de violar o sigilo do voto, capturando as comunicações realizadas entre o terminal do mesário e a urna.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) (X) *Software* Básico da Urna Eletrônica (X) *Software* de Carga (SCUE) (X) *Software* Gerenciador de Aplicativos (GAP) (X) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** (X) Urna eletrônica ( ) Mídias ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias (X) Carga da urna (X) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	360	
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação (X) País	
Conhecimentos necessários para a realização do teste	Linguagens de programação, protocolos de comunicação	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF - 70070-600 - Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 - Horário de funcionamento do protocolo: das 11h às 19h



1

1.1 **2.1 - Descrição geral do teste**

O proponente deverá apresentar uma descrição geral do teste informado.

O objetivo do teste é capturar as informações que trafegam entre o terminal do mesário e a urna, no momento em que é feita a liberação para o eleitor votar através do número de seu título. Isto deve ser feito mediante instalação de um programa que rode em background na urna, durante as eleições. Este programa será responsável por vincular os dados do eleitor com os seus respectivos votos, quebrando assim o sigilo da votação.

1.2 **2.2 - Fundamentação teórica**

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

A fim de liberar a urna para que um eleitor possa votar, o mesário deve digitar, em seu terminal, o número do título de eleitor. Este é recebido pela urna e fica armazenado em sua memória. Se esta informação trafega de forma insegura, um software malicioso poderia ser instalado na urna, a fim de capturar a informação do título de eleitor recebida do terminal do mesário e vinculá-la ao voto que o mesmo eleitor registrasse logo em seguida. Estaria quebrado assim o sigilo da votação.

1.3 **2.3 - Precondições para o teste**

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

Para a realização do teste, são necessários:
- Uma eletrônica
- Terminal do mesário
- Computador
- Pendrive para instalação do software na urna

1.4 **2.4 - Escopo - Superfície de ataque**

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

Escopo do teste: material (urna) e procedimento (votação).

1.5 **2.5 - Janela de atuação simulada do atacante**

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

1.6

Acesso à urna eletrônica nos períodos anterior e posterior à eleição.

2.6 - Pontos de intervenção

1.7

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária de Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

Softwares (instalação de um software para rodar em segundo plano na urna).

1.8

2.7 - Passos a serem realizados e material necessário

1.9

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

1. Atacante identifica o protocolo de comunicação entre o terminal do mesário e a urna.
2. Atacante tem acesso físico à urna.
3. Atacante instala um software malicioso na urna, que ficará rodando em segundo plano durante a eleição.
4. Durante a eleição, o software captura as informações dos eleitores e seus respectivos votos.
5. Após a eleição, atacante tem acesso físico à urna e retira as informações armazenadas pelo software malicioso.
6. Fim.

2.8 - Possíveis resultados e impacto

1.10

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].
- Extensão do ataque. Ex.:
  - uma ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

Quebra do sigilo do voto.

TESTE PÚBLICO DE SEGURANÇA
DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

1.11 **2.9 - Rastreabilidade**

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

Caso os logs da urna sejam armazenados de forma insegura, o atacante poderá apagar os registros de suas atividades, tornando o ataque irrastreável.

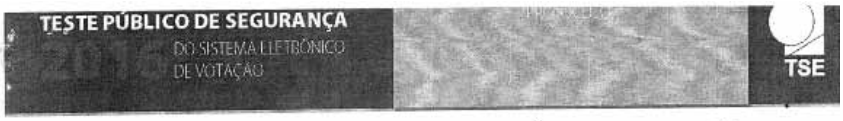
1.12 **2.10 - Solução proposta**

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

Alterar o método de liberação da urna pelo mesário.

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

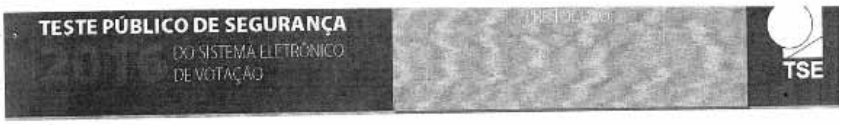
Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h



PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Título do plano de teste	Análise da segurança do armazenamento de arquivos e valores na memória da urna e nas mídias removíveis	
Instituição proponente (se aplicável)		
Responsável	Nome: Charles Figueredo de Barros *E-mail*: charles.barros@ppgi.ufrj.br Telefone (do autor ou responsável): (21) 99288-3429	
Resumo do teste (máximo 120 caracteres)	Analisar os procedimentos de segurança envolvidos na armazenagem de dados na memória e nas mídias removíveis.	
Sistemas afetados	***Softwares*** (X) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) (X) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) (X) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit JE Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** (X) Urna eletrônica (X) Mídias ( ) *Kit JE Connect* **Procedimentos** (X) Geração de mídias (X) Carga da urna ( ) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	360	
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação (X) País	
Conhecimentos necessários para a realização do teste	Linguagens de programação, algoritmos de criptografia	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.



1

1.1 **2.1 - Descrição geral do teste**

O proponente deverá apresentar uma descrição geral do teste informado.

O teste consiste na verificação dos procedimentos de segurança relativos ao armazenamento de dados, tanto na memória da urna quanto nas mídias removíveis. O objetivo é identificar a presença de potenciais vulnerabilidades, tais como:
- Chaves de encriptação/decriptação armazenadas às claras em mídias removíveis ou na memória da urna;
- Chaves de assinaturas digitais armazenadas às claras em mídias removíveis ou na memória da urna;
- Uso de senhas óbvias para proteção de arquivos que armazenam informações sensíveis;
- Arquivo de log armazenado de forma insegura, permitindo sua adulteração na eventualidade de ataques à urna;
- Presença de "contadores de proteção", que armazenam o número total de votos em uma urna, e armazenamento inseguro de tais contadores na memória da urna;
- Uso da mesma chave criptográfica para várias ou todas as urnas.

1.2 **2.2 - Fundamentação teórica**

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

As falhas que este teste busca identificar já foram relatadas na literatura [1,2,3] e podem ser exploradas em diversos tipos de ataque:
- Chaves de encriptação/decriptação armazenadas às claras em mídias removíveis ou na memória da urna: agentes internos com acesso às urnas ou às mídias removíveis poderiam se valer do conhecimento dessas chaves de criptografia para violar o sigilo de informações sensíveis.
- Chaves de assinaturas digitais armazenadas às claras em mídias removíveis ou na memória da urna: assinaturas digitais têm como objetivo garantir a procedência de documentos, arquivos ou programas. Ao armazenar as chaves de assinatura digital de forma insegura, abre-se caminho para que agentes maliciosos sejam capazes de inserir adulterações maliciosas no software da urna de forma indetectável.
- Uso de senhas óbvias para proteção de arquivos que armazenam informações sensíveis: o uso de senhas fracas já foi amplamente criticado na literatura, pois permite os chamados ataques de força bruta, nos quais um adversário ganha acesso indevido a informações sigilosas após diversas tentativas de adivinhar tais senhas. Existem programas que contêm listas com as senhas mais comuns, os chamados "dicionários", que são usados de maneira ostensiva por hackers ao redor do mundo para obter acesso ilícito a redes domésticas ou corporativas, sites e computadores pessoais.
- Arquivo de log armazenado de forma insegura: os arquivos de log registram todos os eventos do sistema, incluindo possíveis ações maliciosas, o que permite que tais ações sejam identificadas e rastreadas posteriormente. Portanto, é fundamental que tais arquivos sejam armazenados de forma segura, caso contrário um agente malicioso poderia obter acesso a este arquivo e apagar os registros de suas ações maldosas, tornando-as indetectáveis e irrastreáveis.
- Presença de "contadores de proteção", que armazenam o número total de votos em uma urna, e armazenamento inseguro de tais contadores na memória da urna: esses contadores, se adulterados, permitem que a contagem dos votos seja alterada de forma maliciosa, beneficiando algum ou alguns candidatos e prejudicando outros. É imprescindível que tais contadores, caso existam, sejam armazenados de forma segura na memória da urna.
- Uso da mesma chave criptográfica para várias ou todas as urnas: tal vulnerabilidade já foi relatada anteriormente. estabelecer uma única chave criptográfica para todas as urnas é o mesmo que trancar vários cofres, que guardam segredos valiosos, com uma única chave. Se um adversário conseguir acesso a esta chave, ele terá em suas mãos os segredos guardados em todos os cofres. Tal prática vai na contramão dos procedimentos de segurança, uma vez que facilita o trabalho de agentes maliciosos em vez de dificultar.

Referências:
[1] Diego F. Aranha, Marcelo Monte Karam, André de Miranda, Felipe Scarel. (in)segurança do voto eletrônico no Brasil / Vulnerabilidades no software da urna eletrônica brasileira. In: Cadernos Adenauer 1/2014: Justiça Eleitoral, 117-133, 2014.
[2] Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, Ka-Ping Yee. Source Code Review of the Sequoia Voting System. July 20, 2007.
[3] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, W. P. Zeller: Source Code Review of the Diebold Voting System. Part of the CA Secretary of State's 2007 Top-To-Bottom Review of CA voting systems

1.3 **2.3 - Precondições para o teste**

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

Para a realização do teste, são necessários:
- Acesso à memória da urna;
- Acesso às mídias removíveis;
- Equipe executora do teste.

1.4 **2.4 - Escopo - Superfície de ataque**

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

Escopo do teste: material (urna e mídias).

1.5 **2.5 - Janela de atuação simulada do atacante**

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

1.6

Acesso à memória da urna ou às mídias removíveis fora do período eleitoral.

1.7 **2.6 - Pontos de intervenção**

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária de Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

Não se aplica.

1.8

1.9 ***2.7* - Passos a serem realizados e material necessário**

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

Não se aplica.

1.10 2.8 - Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].
- Extensão do ataque. Ex.:
  - uma ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

Não se aplica.

1.11 2.9 - Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

Não se aplica.

1.12 2.10 - Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

Adequação dos procedimentos de armazenagem de dados na memória da urna e nas mídias removíveis.

Protocolo	Data	
	Resultado ( ) Aprovado	

	( ) Aprovado com ressalvas ( ) Reprovado

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA
DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Título do plano de teste Análise de práticas de programação relacionadas ao uso de primitivas criptográficas e outros aspectos de segurança no código-fonte	
Instituição proponente (se aplicável)	
Responsável	Nome: Charles Figueredo de Barros *E-mail*: charles.barros@ppgi.ufrj.br Telefone (do autor ou responsável): (21) 99288-3429
Resumo do teste (máximo 120 caracteres)	Análise do código-fonte em busca de possíveis vulnerabilidades decorrentes de práticas de programação inadequadas.
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) (X) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) (X) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) (X) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos (X) Subsistema de Instalação e Segurança (SIS) ***Hardwares*** (X) Urna eletrônica ( ) Mídias ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias ( ) Carga da urna (X) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	360
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação (X) País
Conhecimentos necessários para a realização do teste	Linguagens de programação, algoritmos de criptografia e geração de números aleatórios

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

1

1.1 **2.1 - Descrição geral do teste**

O proponente deverá apresentar uma descrição geral do teste informado.

O teste consiste na varredura do código-fonte em busca de práticas inadequadas de programação, que podem incluir os seguintes itens:
- Uso de primitivas criptográficas: presença de chaves criptográficas definidas estaticamente no código, uso de primitivas obsoletas para encriptação ou hash (resumo criptográfico), uso inseguro de algoritmos de criptografia (uso de vetores de inicialização constantes, modos de operação de cifras de bloco inseguros).
- Uso de geradores de números pseudo-aleatórios inadequados ou inseguros criptograficamente, uso de sementes inseguras.
- Verificação inadequada de integridade do software da urna, permissão para instalação de atualizações sem a devida verificação de autenticidade.
- Geração de logs insuficiente.

1.2 **2.2 - Fundamentação teórica**

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

O uso de práticas inadequadas de programação insere vulnerabilidades que podem ser exploradas por agentes maliciosos. Essas práticas já foram citadas na literatura [1,2,3] e referem-se a:
- Mau uso de primitivas criptográficas: chaves criptográficas definidas estaticamente no código-fonte são vulneráveis, uma vez que agentes internos maliciosos poderiam se valer do conhecimento dessas chaves para violar o sigilo de informações delicadas; o mesmo pode ocorrer em decorrência do uso de primitivas criptográficas obsoletas ou do uso inadequado de algoritmos modernos, como por exemplo o emprego de vetores de inicialização constantes em cifras de bloco, o que possibilita a realização de ataques bem-sucedidos, conforme já foi relatado na literatura.
- Geração insegura de números pseudo-aleatórios: o uso de algoritmos inseguros para geração de números pseudo-aleatórios pode comprometer o sigilo do voto, uma vez que este é baseado na desvinculação entre os dados do eleitor e os dados do seu voto através de processos de randomização. O uso inadequado desta ferramenta possibilita a um agente malicioso a reconstrução do vínculo entre os dados do eleitor e do seu respectivo voto, comprometendo uma das premissas da eleição, que é o sigilo do voto.
- Verificação de integridade inadequada: se o software carregado na urna é responsável por verificar sua própria integridade, sem a presença de um módulo externo de verificação, qualquer software adulterado pode verificar a si mesmo, tornando impossível a detecção de tais adulterações.
- Geração insuficiente de logs: outra vulnerabilidade registrada na literatura, que dificulta o processo de rastreamento de possíveis ações maliciosas, conduzidas por agentes internos ou externos.

Referências:
[1] Diego F. Aranha, Marcelo Monte Karam, André de Miranda, Felipe Scarel. (In)segurança do voto eletrônico no Brasil / Vulnerabilidades no software da urna eletrônica brasileira. In: Cadernos Adenauer 1/2014: Justiça Eleitoral, 117-133, 2014.
[2] Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, Ka-Ping Yee. Source Code Review of the Sequoia Voting System. July 20, 2007.
[3] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, W. P. Zeller: Source Code Review of the Diebold Voting System. Part of the CA Secretary of State's 2007 Top-To-Bottom Review of CA voting systems

1.3 **2.3 - Precondições para o teste**

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que

sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

Para a realização do teste, são necessários:
- Código-fonte da urna;
- Material para anotações;
- Equipe executora do teste;
- Técnicos da equipe de programação do TSE, para auxiliar a encontrar trechos relevantes do código.

1.4 **2.4 - Escopo - Superfície de ataque**

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:
- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

Escopo do teste: Código-fonte.

1.5 **2.5 - Janela de atuação simulada do atacante**

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

1.6

Acesso ao código-fonte da urna fora do período eleitoral.

1.7 **2.6 - Pontos de intervenção**

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária de Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

Não se aplica.

1.8

1.9 **2.7 - Passos a serem realizados e material necessário**

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

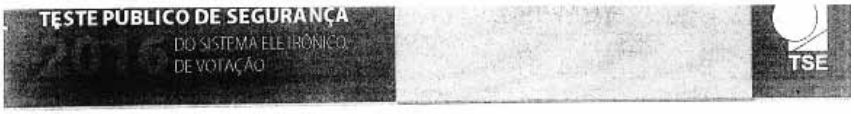
A seguir, um exemplo de lista de passos:
1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

Não se aplica.



1.10 **2.8 - Possíveis resultados e impacto**

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].
- Extensão do ataque. Ex.:
  - urna ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

Não se aplica.

1.11 **2.9 - Rastreabilidade**

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

Não se aplica.

1.12 **2.10 - Solução proposta**

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

Adequação do código-fonte a boas práticas de programação.

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Grupo 4

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste Tentativa de fraude na destinação dos votos		
Instituição proponente (se aplicável) Pessoa Física		
Responsável	Nome: Elisabete Evaldt (Grupo 4) *E-mail*: elisabete@aneel.gov.br Telefone (do autor ou responsável): (61) 9811-1087	
Resumo do teste (máximo 120 caracteres)	Tentativa de fraude na destinação dos votos na urna através de controle dos dispositivos de teclado e impressora.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) (X) *Software* Básico da Urna Eletrônica (X) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit JE Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** [ ] Urna eletrônica [X] Mídias [ ] *Kit JE Connect* ***Procedimentos*** ( ) Geração de mídias (X) Carga da urna ( ) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	6 horas	
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação (X) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimento do processo eleitoral e material produzido nos diversos momentos de uma eleição. Conhecimento prévio do código-fonte dos sistemas afetados.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O proponente deverá apresentar uma descrição geral do teste informado.

O grupo tentará explorar um possível acesso indevido à mídia de carga da urna eletrônica, no intuito de inserir/alterar o conteúdo de forma a permitir uma tentativa de fraude na destinação dos votos através de controle dos dispositivos de teclado e impressora.

2.2 – Fundamentação teórica

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

O objetivo é atender ao Edital do Teste Público de Segurança cujo escopo é o sistema eletrônico de votação que será utilizado nas eleições municipais de 2016. Conforme Resolução TSE nº 23.444, de 30 de abril de 2015, o intuito do plano de teste é o de violar a destinação dos votos.

2.3 – Precondições para o teste

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

O teste requer a simulação de uma eleição previamente configurada pelo TSE (cargos e candidatos) e a geração de uma mídia de carregamento. O TSE deverá entregar a mídia para o grupo, juntamente com o cabo conector USB, simulando o acesso indevido pelo ator do ataque.
O grupo solicita a autorização para utilização de notebooks próprios com sistema operacional Linux, conectados à Internet, configurados pelos próprios investigadores. O TSE poderá realizar auditoria e acompanhamento de todas as ações feitas pelos investigadores nessas máquinas sem restrições. A intenção é simular a realidade de um ataque caso a mídia de carga seja exposta à um ator mal-intencionado após ser gravada e antes de ser usada para carregar a urna.

2.4 – Escopo – Superfície de ataque

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

Mídia de Carga da Urna Eletrônica.

2.5 – Janela de atuação simulada do atacante

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

Acesso à memória de carga gerada.

2.6 – Pontos de intervenção

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária de Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

Em caso de ataque bem sucedido à mídia de carga, o ataque deverá intervir na comunicação interna com a impressora e com o teclado do terminal do eleitor.

2.7 – Passos a serem realizados e material necessário

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

Atacante tem acesso físico à mídia de carga da urna, após ser gerada e antes de ser utilizada na urna eletrônica;
Utilizando um computador portátil, lê a mídia de carga no intuito de violar o sigilo das partições de arquivos;
Atacante recupera arquivos do sistema operacional da urna e substitui partes de suas instruções;
6 horas
A mídia deverá ser usada normalmente para carregamento da urna pelo TSE sem acusar a violação;

2.8 – Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].
- Extensão do ataque. Ex.:
  - urna ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

O ataque na alteração do destino do voto terá abrangência na urna eletrônica durante o processo de votação na seção eleitoral. Caso a mídia seja carregada com sucesso na urna, a probabilidade de sucesso aumentará de acordo com o número de votos registrados na votação.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

2.9 – Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

Caso suceda, o ataque somente será rastreável caso haja auditoria aleatória de código do sistema operacional na uma eletrônica.

2.10 – Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o Investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

Não há conhecimento suficiente do processo eletrônico de votação para formular uma solução no momento.

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

Grupo 5

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — PROTOCOLO: — TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual		
Instituição proponente (se aplicável) Universidade de Taubaté		
Responsável	Nome: Luis Fernando de Almeida *E-mail*: luis.almeida@unitau.br Telefone (do autor ou responsável): (12) 3629-5982	
Resumo do teste (máximo 120 caracteres)	Um princípio primário do TSE é garantir o direito do voto a todo cidadão, incluindo aqui, aquelas pessoas com deficiência visual. Nesse sentido, as urnas eletrônicas disponibilizam de recurso de áudio a fim de também proporcionar a inclusão social desses cidadãos. Basicamente, consiste de um fone de ouvido no qual o deficiente visual, ao digitar uma tecla identificada por impressão em braile, pode ouvir o número digitado, ratificando sua opção de voto. A ideia consiste em tentar obter e gravar, por meio desta saída de áudio, a sequência de todas as teclas digitadas durante a votação e, consequentemente, quebrar o sigilo do voto. O sigilo dos votos da eletrônica seria quebrado por meio do acompanhamento da ordem dos votantes da respectiva seção eleitoral.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) (x) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** (x) Urna eletrônica (x) Mídias ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias ( ) Carga da urna (x) Votação ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	60 minutos	
Extensão do ataque	(x) Urna ou seção eleitoral (x) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Hardware, programação, Arduino/Raspberry Pi, *bluetooth*.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O proponente deverá apresentar uma descrição geral do teste informado.

O teste em questão consiste em acoplar algum tipo de dispositivo, por exemplo, Arduino/Raspberry Pi, o qual possibilite capturar o áudio disponibilizado para deficientes visuais e armazenar e alguma mídia para posterior recuperação e identificação da sequência da votação de uma dada urna eletrônica. Paralelamente, obtém-se a ordem dos eleitores que votaram na respectiva seção eleitoral. Com as duas informações em mãos, pretende-se quebrar o sigilo do voto, ou seja, mapear o voto de cada eleitor.

2.2 – Fundamentação teórica

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

O teste concentra-se em um dos conceitos primários relacionados à multimídia dos computadores: o áudio (saída e gravação). Uma saída de áudio, ao mesmo tempo em que proporciona ouvir arquivos de sons, pode ser utilizada para se gravar esses sons por meio de um dispositivo que funcione como um "microfone" e capture-os e armazene-os em outros dispositivos, ou mesmo, transmita-os por meio de *bluetooth* para algum dispositivo nas proximidades.

2.3 – Precondições para o teste

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

Recursos materiais:
- urna eletrônica.
- Arduino/Raspberry Pi.

Recursos de software:
- compilador C/C++.
- ambiente de desenvolvimento Java.
- internet para possíveis consultas sobre programação e Arduino.

Relaxamentos de procedimentos-padrão:
- Não verificação adequada da saída de áudio da urna eletrônica.

2.4 – Escopo – Superfície de ataque

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

2.5 – Janela de atuação simulada do atacante

A alteração está relacionada ao acoplamento de dispositivo para captura de áudio na parte traseira da urna eletrônica.

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

O atacante terá sua atuação no acesso à urna eletrônica, após sua instalação nas respectivas dependências das seções eleitorais pela equipe do tribunais regionais.

2.6 – Pontos de intervenção

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária da Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

O principal ponto de intervenção é o relacionado a não verificação devida da saída da áudio, constantemente, que possibilita, em um dado momento o acoplamento do dispositivo em questão.

2.7 – Passos a serem realizados e material necessário

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

1. O atacante tem acesso à urna eletrônica.
2. O atacante acopla o dispositivo na saída de áudio da urna.
3. Inicia-se a votação.
4. Dispositivo captura e grava os dados de áudio.
5. Elemento externo (pessoa) acompanha a ordem dos eleitores que estão votando.
6. Último eleitor vota.
7. Dispositivo é retirado da urna.
8. Áudios gravados são transformados em votos pelo processo simples de ouvir a gravação.
9. Sequência dos votos é mapeada com a sequência dos eleitores.

2.8 – Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].

- Extensão do ataque. Ex.:
  - urna ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

Resultado esperado: quebra do sigilo do voto. Extensão do ataque: urna ou seção eleitoral.

2.9 – Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

O teste pressupõe, em um dado momento, a ausência de uma verificação adequada da saída de áudio da urna eletrônica por parte da equipe de uma determinada seção eleitoral proporcionando o acoplamento do dispositivo de captura e gravação de áudio.

2.10 – Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Individual – João Felipe Souza

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste **DESTRUIDOR DE VOTOS**		
Instituição proponente (se aplicável)		
Responsável	Nome: ***João Felipe Souza*** *E-mail*: **joaofelipe@iftm.edu.br** Telefone (do autor ou responsável): **(38) 99975-7258**	
Resumo do teste (máximo 120 caracteres)	Teste para explorar o controle de transação da urna e destruir votos depois do registro de comparecimento dos eleitores.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) **(X) *Software* de Votação (Vota)** ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** **(X) Urna eletrônica** ( ) Mídias ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias ( ) Carga da urna **(X) Votação** ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	**45 minutos**	
Extensão do ataque	**(X) Urna ou seção eleitoral** ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimentos básicos em eletrônica. Conhecimentos avançados em Sistema Operacional Linux.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

Para garantir a consistência do sistema eleitoral brasileiro é necessário destinar esforços para manter a integridade dos votos e, além disso, que se mantenha o anonimato dos votos. A integridade dos votos é importante para garantir o bom funcionamento de todo o processo eleitoral. Um dos meios de se verificar a integridade dos votos é se verificando os resultados apresentados nos boletins de urna. O total de eleitores comparecidos deve corresponder ao total de votos computados.

Este teste de segurança consiste na tentativa de explorar uma falha no software da urna eletrônica possibilitando a quebra da integridade do voto eletrônico. Para tanto, será utilizado dispositivo radiocontrolado para desligar a urna eletrônica no momento da escrita de um voto, resultando no registro do comparecimento de um eleitor sem que seja registrado o seu voto. Esta quebra de integridade poderá comprometer todos os outros votos registrados na urna, uma vez que o número de comparecimentos não será igual ao número de votos computados. Este ataque, se bem sucedido, poderá destruir o voto de um eleitor impedindo o seu registro, embora seja computado o seu comparecimento, ou seja, desviando o voto do eleitor do candidato escolhido para nenhum.

2.2 – Fundamentação teórica

O controle de transação tem o objetivo de garantir que uma operação sobre um conjunto de dados seja realizada de forma consistente e permanente. O processo de registro de um voto na urna eletrônica passa por algumas etapas como o registro do comparecimento do eleitor e o registro do voto do eleitor. Caso estas etapas não sejam realizadas protegidas por um controle de transação eficiente poderão ocorrer falhas no processo de escrita, resultando em registro de um comparecimento sem registro de voto.

2.3 – Precondições para o teste

Para a realização do "Teste I" será necessário a utilização de um dispositivo de hardware radiocontrolado capaz de interromper o fornecimento de energia elétrica para a fonte de alimentação da urna eletrônica. O dispositivo será conectado em uma extremidade com o polo positivo da bateria e na outra extremidade com cabo que fornece energia para a fonte de alimentação, criando uma unidade de intermediação do fornecimento de energia. Este dispositivo será disponibilizado pelo investigador.

O teste será realizado pelo investigador João Felipe Souza, Professor E. B. T. T. De Informática do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro – Campus Paracatu. O investigador possui graduação em Ciência da Computação / UFV 2007 e Mestrado em Engenharia Agrícola com Ênfase em Recursos Hídricos e Ambientais / UFV 2011.

2.4 – Escopo – Superfície de ataque

O teste prevê uma atuação material no hardware da urna eletrônica. Para a realização do teste será necessário obter acesso ao interior do compartimento da bateria interna para introdução de um dispositivo radiocontrolado. Como resultado do ataque ao hardware da urna será provocado uma falha no software de registro dos votos.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

2.5 – Janela de atuação simulada do atacante

O teste se baseia em um ataque no qual o atacante precisa ter acesso a uma eletrônica antes das eleições para inserir o dispositivo radiocontrolado e depois das eleições para remover o dispositivo. Além disso, o atacante deve interromper o fornecimento de energia na seção no instante em que for aplicar o ataque.

2.6 – Pontos de intervenção

Para a realização do teste é necessário a intervenção no hardware da urna eletrônica com a finalidade de se instalar um dispositivo radiocontrolado para desligar a urna eletrônica.

2.7 – Passos a serem realizados e material necessário

O Teste será realizado seguindo-se os seguintes passos:

1. Atacante obtém acesso a urna antes das eleições. 5 min.
2. Atacante insere dispositivo eletrônico radiocontrolado na bateria interna da urna. 5 min.
3. Atacante prepara ambiente e interrompe o fornecimento de energia elétrica da seção. 10 min.
4. Atacante acessa a cabina de votação para votar. 10 min.
5. Atacante aciona mecanismo para desligar a urna no momento da gravação do seu voto. 5 min.
6. Urna registra o comparecimento, mas não registra o voto, o teste foi bem sucedido. 5.
7. Atacante obtém acesso a urna depois das eleições para remover mecanismo radiocontrolado. 5
8. Fim do teste.

Tempo de duração do teste: 45 minutos.

2.8 – Possíveis resultados e impacto

Espera-se que a plena execução deste ataque possa resultar no mal funcionamento da urna, resultando na gravação de um comparecimento e na não gravação de um voto. Com esta falha a integridade dos dados será comprometida e todos os votos da urna deverão ser descartados. O ataque tem extensão a urna ou seção eleitoral. A probabilidade de sucesso do ataque depende do alcance do mecanismo de transação dos aplicativos da urna eletrônica.

2.9 – Rastreabilidade

O teste não pode ser rastreado porque não altera nenhuma característica da urna e também não viola qualquer lacre de segurança.

2.10 – Solução proposta

Caso seja bem sucedido, este tipo de ataque pode ser evitado aperfeiçoando-se o sistema eletrônico de transação dos aplicativos da urna eletrônica.

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste **REGISTRADOR DO TECLADO**		
Instituição proponente (se aplicável)		
Responsável	Nome: ***João Felipe Souza*** *E-mail*: **joaofelipe@iftm.edu.br** Telefone (do autor ou responsável): **(38) 99975-7258**	
Resumo do teste (máximo 120 caracteres)	Teste para quebrar o sigilo do voto introduzindo dispositivo para registro das teclas digitadas na urna eletrônica.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** **(X) Urna eletrônica** ( ) Mídias ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias ( ) Carga da urna **(X) Votação** ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	**120 minutos**	
Extensão do ataque	**(X) Urna ou seção eleitoral** ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimentos básicos em eletrônica. Conhecimentos avançados em Sistema Operacional Linux.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

Para garantir a consistência do sistema eleitoral brasileiro é necessário destinar esforços para manter a integridade dos votos e, além disso, que se mantenha o anonimato dos votos. A quebra do sigilo dos votos pode causar uma série de consequências graves ao processo democrático de escolha dos votos e comprometer os resultados de uma eleição.

Este teste de segurança consiste na tentativa de explorar uma vulnerabilidade de segurança no sistema eleitoral possibilitando a quebra do sigilo do voto eletrônico. Para tanto, serão utilizados dispositivos registradores de teclado.

Para segmentar os trabalhos serão apresentadas três alternativas de testes:

Teste I - Introdução de dispositivo registrador de teclas via porta USB
Teste II - Introdução de teclado alternativo
Teste III - Conexão de teclado virtual simulado

Teste I. Introdução de dispositivo registrador de teclas via porta USB

Este teste se baseia na introdução no hardware da urna de um dispositivo capaz de registrar as teclas digitadas no teclado do terminal do eleitor. O dispositivo será construído ou adquirido de modo que ofereça funcionalidades para armazenar tudo o que for digitado no teclado e/ou transmitir em tempo real ou não para outro dispositivo receptor. A conexão será realizada por meio da porta USB da placa mãe da urna eletrônica intermediando a conexão entre a placa-mãe e o teclado. Para se proteger a urna precisa ser capaz de detectar estes elementos estranhos e interromper a sua inicialização.

Teste II - Introdução de teclado alternativo

Teste baseado no estudo da possibilidade de substituição do teclado original da urna eletrônica por um teclado alternativo que hipoteticamente poderia conter, embutido no seu hardware, elementos para registrar e transmitir tudo o que se digita no teclado. Para se proteger a urna precisa ser capaz de detectar a substituição do teclado original e abortar a inicialização.

Teste III - Conexão de teclado virtual simulado

Este é um teste alternativo que visa a criação de um teclado virtual no Sistema Operacional Linux que, conectado com a placa-mãe da urna eletrônica via porta USB poderia ser capaz de enganar a urna eletrônica se passando por um falso teclado e sendo reconhecido normalmente. Obviamente que se trata de um teste de terceira via para o caso em que os Teste I e Teste II sejam detectados e impedidos pela urna. O objetivo do Teste III é demonstrar a possibilidade de criação de um teclado rastreado similar ao teclado original.

2.2 - Fundamentação teórica

Este teste está fundamentado na hipótese de obtenção dos dados diretamente na entrada da urna eletrônica e antes mesmo de serem recebidos pelo Linux UENUX e pelo aplicativo VOTA. Esta técnica de obtenção dos dados é descrita por Weidman (2014) como a utilização de um registrador de teclas como maneira de permitir que o próprio usuário forneça as informações desejadas.

Apesar da abordagem utilizando um dispositivo físico é importante salientar que os registradores de teclas podem ser implementados em hardware ou software. O motivo da escolha por uma implementação via hardware é justamente a impossibilidade de introdução de código malicioso no sistema operacional.

Referências: WEIDMAN, Georgia. Testes de Invasão: uma introdução prática ao hacking. São Paulo: Editora Novatec, 2014.

2.3 – Precondições para o teste

Para a realização do "Teste I" será necessário a utilização de um dispositivo de hardware capaz de registrar tudo o que for digitado no teclado da urna eletrônica. O dispositivo registrador do teclado será conectado em uma extremidade com o teclado e na outra extremidade com a placa mãe, criando uma unidade de intermediação da comunicação entre a placa mãe e o teclado. Este dispositivo será disponibilizado pelo investigador.

Para o "Teste II" será necessário utilizar um teclado USB padrão, que será conectado na placa mãe em substituição ao teclado original do terminal do eleitor. Poderá ser necessário alterar o conector USB do teclado para que seja possível conectá-lo a placa mãe.

Para o "Teste III" será utilizado um computador instalado com o Sistema Operacional Linux (disponibilizado pelo TSE com acesso de superusuário), com uma entrada USB disponibilizada para leitura do teclado do terminal do eleitor e parametrização de um teclado virtual. É necessário a utilização do compilador gcc. Também será necessário a utilização de um cabo USB Macho X Macho(fornecido pelo investigador) para conexão entre o computador e a Urna Eletrônica.

Para a execução dos três testes será necessário o relaxamento das condições de segurança adotadas e recomendadas pelo TSE com a finalidade de romper os lacres de segurança da urna eletrônica. Além disso, será necessário que existam demais pessoas corrompidas a participar do ataque.

O teste será realizado pelo investigador João Felipe Souza, Professor E. B. T. T. De Informática do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro – Campus Paracatu. O investigador possui graduação em Ciência da Computação / UFV 2007 e Mestrado em Engenharia Agrícola com Ênfase em Recursos Hídricos e Ambientais / UFV 2011.

2.4 – Escopo - Superfície de ataque

O teste prevê uma atuação material no hardware da terminal do eleitor da urna eletrônica. Para a realização do teste será necessário obter acesso ao interior da urna para introdução de um dispositivo de hardware.

Além disso, os lacres serão violados e o procedimento de verificação dos lacres deve permitir a continuidade da realização do teste, mesmo que a violação seja identificada em uma etapa posterior as eleições.

2.5 – Janela de atuação simulada do atacante

O teste se baseia em um ataque no qual o atacante precisa ter acesso a uma eletrônica antes das eleições para inserir o dispositivo de hardware para registros das teclas e depois das eleições para remover o dispositivo.

2.6 – Pontos de intervenção

Para a realização do teste é necessário a intervenção no hardware da uma eletrônica com a finalidade de se instalar um dispositivo alternativo e não original. Caso o sistema eletrônico não seja capaz de identificar este hardware estranho o teste será bem sucedido.

2.7 – Passos a serem realizados e material necessário

O Teste I será realizado seguindo-se os seguintes passos:

1. Atacante tem acesso físico a urna eletrônica antes das eleições. 1 min.

2. Atacante viola os lacres de segurança. 5 min.
3. Atacante abre a urna eletrônica . 15 min.
4. Atacante introduz o dispositivo eletrônico para registro do teclado. 15 min.
5. Atacante fecha a urna. 15 min.
6. Atacante reposiciona os lacres de segurança. 5 min.
7. Durante as eleições o atacante registra a ordem de votação dos eleitores. 20 min.
8. Atacante obtém acesso a urna eletrônica após a realização das eleições. 15 min.
9. Atacante realiza a retirada do dispositivo eletrônico de registro do teclado e obtém sequência de votação. 30 min.
10. Fim do Teste I

Tempo total: 121 minutos.

O Teste II será realizado seguindo-se os seguintes passos:

1. Atacante tem acesso físico a urna eletrônica antes das eleições. 1 min.
2. Atacante viola os lacres de segurança. 5 min.
3. Atacante abre a urna eletrônica . 15 min.
4. Atacante substitui teclado original por outro teclado USB. 25 min.
5. Atacante fecha a urna. 15 min.
6. Atacante reposiciona os lacres de segurança. 5 min.
7. Durante as eleições o atacante registra a ordem de votação dos eleitores. 20 min.
8. Atacante obtém acesso a urna eletrônica após a realização das eleições. 15 min.
9. Atacante realiza a retirada do dispositivo eletrônico de registro do teclado e obtém sequência de votação. 30 min.
10. Fim do Teste II
11. Tempo total: 131 minutos.

O Teste III será realizado seguindo-se os seguintes passos:

1. Atacante tem acesso físico a urna eletrônica antes das eleições. 1 min.
2. Atacante viola os lacres de segurança. 5 min.
3. Atacante abre a urna eletrônica . 15 min.
4. Atacante conecta o teclado da urna no computador via porta USB para obter padrões a parâmetros de configuração do teclado virtual. 25 min.
5. Atacante substitui teclado original por uma conexão USB com a máquina para conexão do teclado virtual, hipoteticamente seria um teclado fisicamente idêntico ao teclado original da urna. 25 min.
6. Atacante fecha a urna. 15 min.
7. Atacante inicia a urna eletrônica e, caso seja iniciado normalmente o teste será bem sucedido. 14
8. Fim do Teste III

Tempo total: 100 minutos.

2.8 – Possíveis resultados e impacto

Espera-se que a plena execução deste ataque possa resultar na quera do sigilo do voto. O ataque tem extensão a urna ou seção eleitoral. A probabilidade de sucesso do ataque depende do alcance do mecanismo de verificação de hardware da urna eletrônica.

2.9 – Rastreabilidade

O mecanismo de segurança que garante a proteção contra este tipo de ataque são os lacres. Caso exista alguma forma para substituir os lacres danificados por novos lacres intactos a rastreabilidade será prejudicada. O ataque pode ser descoberto caso seja identificado a violação de algum lacre.

2.10 – Solução proposta

Caso seja bem sucedido, este tipo de ataque pode ser evitado aperfeiçoando-se o sistema eletrônico de verificação do hardware de modo a não permitir a conexão de hardware externo.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — PROTOCOLO — TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste **ROOT KIT JE CONNECT**		
Instituição proponente (se aplicável)		
Responsável	Nome: ***João Felipe Souza*** *E-mail*: **joaofelipe@iftm.edu.br** Telefone (do autor ou responsável): **(38) 99975-7258**	
Resumo do teste (máximo 120 caracteres)	Teste para explorar possível vulnerabilidade no kit JE Connect e obter acesso ao RECArquivos e InfoArquivos.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) **(X) Sistemas transportadores** **(X) *Kit* JE *Connect*** **(X) RecArquivos** **(X) InfoArquivos** ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** ( ) Urna eletrônica ( ) Mídias **(X) *Kit* JE *Connect*** **Procedimentos** ( ) Geração de mídias ( ) Carga da urna ( ) Votação **(X) Transmissão de arquivos**
Duração estimada do teste (em minutos)	**140 minutos**	
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação **(X) País**	
Conhecimentos necessários para a realização do teste	Conhecimentos avançados em Sistema Operacional Linux.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O teste consiste na tentativa de execução de código malicioso dentro do kit JE Connect para se obter acesso ao transportador e à VPN (Virtual Private Network) de transmissão de dados. Uma possível falha de segurança poderia levar ao comprometimento da integridade do voto no que diz respeito ao seu destino. Alterações nesta fase, depois da impressão do boletim de urna (BU), podem ser facilmente detectadas mediante a comparação do BU com os dos dados disponibilizados pelo TSE. Apesar disso, é necessário validar o sistema contra vulnerabilidades nesta fase do processo com a finalidade de se preservar a boa fé pública no sistema eleitoral, uma vez que falhas em qualquer etapa do processo podem causa desconfiança em todo o processo.

Uma vez garantido o acesso ao kit JE Connect e à VPN, serão executados testes de penetração com o objetivo de se estabelecer um ponto crítico para ser explorado nos softwares RECArquivos e InfoArquivos. Havendo vulnerabilidades o teste será bem sucedido.

2.2 – Fundamentação teórica

A exploração de falhas e vulnerabilidades é um mecanismo muito empregado por Hackers para invasão de sistemas. Segundo Weidman (2014), a fase de análise de vulnerabilidades visa determinar até que ponto as estratégias de exploração de falhas poderão ser bem sucedidas. Além disso, a autora salienta que, embora eficazes, os scanners de vulnerabilidade não podem substituir totalmente o raciocínio crítico, portanto, deve-se realizar análises manuais em busca de vulnerabilidades.

O Metasploit é uma ferramenta padrão para os testes de invasão e permite a verificação por uma base de dados de vulnerabilidade, além de permitir a criação de novos sploits.

O acesso ao kit JE Connect poderá expor uma parte do sistema eleitoral a ameaças de códigos maliciosos e e permitir acesso exclusivo ao computador e suas informações. Uma backdoor pode ser aberta se um usuário mal intencionado obter acesso às mídias que contém o kit.

Referências bibliográficas: WEIDMAN, Georgia. Testes de invasão: uma introdução prática ao hacking. São Paulo: Editora Novatec, 2014.

2.3 – Precondições para o teste

Para a realização do será necessário a utilização de um computador instalado com Sistema Operacional Linux (cedido pelo TSE). Além disso, será necessário a utilização de dois pen-drivers para cópia do kit JE Connect.

O teste será realizado pelo investigador João Felipe Souza, Professor E. B. T. T. De Informática do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro – Campus Paracatu. O investigador possui graduação em Ciência da Computação / UFV 2007 e Mestrado em Engenharia Agrícola com Ênfase em Recursos Hídricos e Ambientais / UFV 2011.

2.4 – Escopo – Superfície de ataque

O teste prevê uma atuação no sotware do kit JE Connect e no servidor de aplicações RecArquivos e InfoArquivos. Para a realização do teste será necessário obter acesso ao kit JE Conenct para se inserir código malicioso. Como resultado do ataque ao software será possível alterar a destinação dos votos.

2.5 – Janela de atuação simulada do atacante

O teste se baseia em um ataque no qual o atacante precisa ter acesso a mídia que contém o kit JE Connect antes das eleições para inserir o código malicioso.

2.6 – Pontos de intervenção

Para a realização do teste é necessário a intervenção no software da urna eletrônica com a finalidade de se instalar um código malicioso para se obter acesso a VPN por meio do kit JE Connect.

2.7 – Passos a serem realizados e material necessário

O Teste será realizado seguindo-se os seguintes passos:

1. Atacante obtém acesso ao pen-drive do kit JE Connect e ao pen-drive da chave. 5 min.
2. Atacante utiliza o comando dd e realiza uma cópia dos dois pen-drivers. 20 min.
3. Efetua-se a montagem da imagem do pen-drive do kit JE Connect. 5 min.
4. Efetua-se a alteração da imagem do Linux, inserindo um rootkit com backdoor. 10 min.
5. Inicializa-se o kit JE Connect em uma máquina virtual. 10 min.
6. Realiza-se o acesso remoto ao kit JE Connect, via código malicioso previamente inserido. 5 min.
7. Obtém-se acesso à VPN de transmissão de dados. 5 min.
8. Realiza-se teste de penetração no servidor RecArquivos e InfoArquivos. 60 minutos.
9. Explora-se vulnerabilidades (se encontradas) e altera-se os votos. 20 min.
10. Fim do teste.

Tempo de duração do teste: 140 minutos.

2.8 – Possíveis resultados e impacto

Espera-se que a plena execução deste ataque possa resultar na possibilidade de alteração dos votos no servidor. Com esta falha a integridade dos dados será comprometida. O ataque tem extensão nacional. A probabilidade de sucesso do ataque depende dos mecanismos de segurança existentes no kit JE Connect e no servidor.

2.9 – Rastreabilidade

O teste não pode ser rastreado porque não altera nenhuma característica da urna e também não viola qualquer lacre de segurança. Entretanto, a alteração do resultado das eleições poderá ser descoberta por meio de simples conferência dos boletins de urna.

2.10 – Solução proposta

Caso seja bem sucedido, este tipo de ataque pode ser evitado aperfeiçoando-se o sistema eletrônico de segurança do kit JE Connect e do servidor RecArquivos e InfoArquivos.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — PROTOCOLO — TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste **REFLASH DE URNA**		
Instituição proponente (se aplicável)		
Responsável	Nome: ***João Felipe Souza*** *E-mail*: **joaofelipe@iftm.edu.br** Telefone (do autor ou responsável): **(38) 99975-7258**	
Resumo do teste (máximo 120 caracteres)	Teste para explorar possível vulnerabilidade no processo de carga da urna e realizar eleições simuladas e direcionadas.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica **(X) *Software* de Carga (SCUE)** ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** **(X) Urna eletrônica** **(X) Mídias** ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias **(X) Carga da urna** **(X) Votação** ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	**75 minutos**	
Extensão do ataque	**(X) Urna ou seção eleitoral** ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimentos avançados em Sistema Operacional Linux.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O teste consiste em obter uma imagem clone da flash de carga para "re-flashear" a urna eletrônica depois da realização das eleições e realizar uma eleição simulada direcionando-se os votos.

Depois da realização das eleições, e de posse da lista de eleitores que compareceram para votar, teoricamente é possível realizar uma eleição simulada e inserir os mesmos títulos eleitorais, entretanto, direcionando os votos para um determinado candidato.

Para realizar esta segunda eleição será necessário obter um clone da memória de carga da urna eletrônica para que seja possível realizar novo procedimento de carga e reiniciar o processo eleitoral. Além disso, é necessário haver pessoas corrompidas no processo para substituição do boletim de urna impresso.

2.2 – Fundamentação teórica

Um importante mecanismo de segurança do sistema eleitoral é a lista de comparecimento dos eleitores. Por meio desta lista é possível saber quais eleitores compareceram ou não a uma eleição e, deste modo, é possível identificar uma fraude eleitoral simplesmente comparando esta lista com a lista de justificativas, se um eleitor votou em uma determinada seção, e justificou em outra já existe o indício de ocorrência de falhas no processo eleitoral. Pensando nisso, o teste visa simular uma eleição falsa inserindo o número do título eleitoral dos mesmos eleitores que compareceram para votar.

A imagem da memória flash para carga inicial da urna, gerada no sistema GEDAI, é empregada para realização da carga inicial da urna eletrônica. Nesta memória flash estão contidas as informações a respeito do pleito ao qual será empregada a urna eletrônica. Teoricamente, a cópia desta memória também permite realizar uma nova carga na mesma urna e, se possível, corresponderá a uma vulnerabilidade que poderá ser explorada.

O ambiente de trabalho do Sistema Operacional Linux disponibiliza o programa dd, que é capaz de realizar cópias "clones" de dispositivos de blocos de armazenamento como pen-drivers e memórias flash. Para executar este comando para copiar uma flash card é necessário permissões de acesso de superusuário.

2.3 – Precondições para o teste

Para a realização do será necessário a utilização de um computador instalado com Sistema Operacional Linux com acesso root (cedido pelo TSE). Além disso, será necessário a utilização de um leitor de flash card compatível com a mídia de armazenamento da urna eletrônica (flash de carga). É importante haver um relaxamento nas condições de segurança recomendadas pelo TSE com a finalidade de se obter tempo para repetição da eleição e também para haver a substituição dos boletins de urna.

O teste será realizado pelo investigador João Felipe Souza, Professor E. B. T. T. De Informática do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro – Campus Paracatu-MG. O investigador possui graduação em Ciência da Computação / UFV 2007 e Mestrado em Engenharia Agrícola com Ênfase em Recursos Hídricos e Ambientais / UFV 2011.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

2.4 – Escopo – Superfície de ataque

O teste prevê uma atuação na flash de carga, na memória de resultados e na urna eletrônica. Para a realização do teste será necessário obter acesso a mídia da flash de carga e da memória de resultados, bem como obter acesso a urna eletrônica após a realização das eleições.

2.5 – Janela de atuação simulada do atacante

O teste se baseia em um ataque no qual o atacante precisa ter acesso a mídia da flash de carga antes e após as eleições. Além disso, é necessário se ter um tempo disponível para realizar as eleições simuladas utilizando-se a mesma urna empregada na eleição verdadeira.

2.6 – Pontos de intervenção

Para a realização do teste é necessário a intervenção no hardware da urna eletrônica com a finalidade de se obter as imagens da flash de carga e da memória de resultados.

***2.7* – Passos a serem realizados e material necessário**

O Teste será realizado seguindo-se os seguintes passos:

1. Atacante obtém acesso ao flash de carga e a memória de resultados da urna, antes das eleições. 5 min.
2. Atacante realiza cópia da flash de carga e da memória de resultados para uma imagem no computador através de cópia bloco a bloco (dd). 10 min.
3. Atacante realiza tentativa de boot com a flash de carga em uma máquina virtual para verificar a possibilidade de se obter acesso ao sistema de arquivos do UENUX. 10 min.
4. Procede-se normalmente as eleições.
5. Ao término das eleições, já de posse do livro com os eleitores presentes, realiza-se o processo inverso ao passo 2, agora voltando para a memória externa a imagem da flash de carga e para a memória de resultados. 20 min.
6. Realiza-se novo procedimento de carga da mesma urna eletrônica.
7. Realiza-se procedimento simulado de votação com a urna eletrônica, desta vez, direcionando-se os votos. 20min.
8. Procede-se ao envio dos dados normalmente. 10 min.
9. Fim do teste.

Tempo de duração do teste: 75 minutos.

2.8 – Possíveis resultados e impacto

Espera-se que a plena execução deste ataque possa resultar na possibilidade de alteração dos votos dos eleitores. Com esta falha a integridade dos dados será comprometida. O ataque tem extensão em nível de uma urna ou seção. A probabilidade de sucesso do ataque depende dos mecanismos de segurança existentes na urna eletrônica.

2.9 – Rastreabilidade

O teste não pode ser rastreado verificando-se os arquivos de log da urna e constatando-se uma votação em horário reduzido.

2.10 – Solução proposta

Caso seja bem sucedido, este tipo de ataque pode ser evitado aperfeiçoando-se o sistema eletrônico de segurança da urna eletrônica com a finalidade de se estabelecer, por exemplo, um log permanente de eventos.

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — PROTOCOLO — TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste **SEQUENCIADOR DE VOTOS**		
Instituição proponente (se aplicável)		
Responsável	Nome: João Felipe Souza *E-mail*: joaofelipe@iftm.edu.br Telefone (do autor ou responsável): (38) 99122-8595	
Resumo do teste (máximo 120 caracteres)	Realizar a quebra do sigilo do voto através de gravações sequenciais dos arquivos de registro de comparecimento do eleitor e do registro digital do voto.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica ( ) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) ( ) Sistemas transportadores ( ) *Kit* JE *Connect* ( ) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** **(X) Urna eletrônica** **(X) Mídias** ( ) *Kit* JE *Connect* **Procedimentos** ( ) Geração de mídias **(X) Carga da urna** **(X) Votação** ( ) Transmissão de arquivos
Duração estimada do teste (em minutos)	40 minutos	
Extensão do ataque	**(X) Urna ou seção eleitoral** ( ) Local de votação ( ) Zona eleitoral ( ) Município ( ) Unidade da Federação ( ) País	
Conhecimentos necessários para a realização do teste	Conhecimentos avançados em sistema operacional Linux.	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

DETALHAMENTO DO TESTE

2.1 – Descrição geral do teste

O teste consiste na quebra do sigilo do voto por meio de gravações sequenciais do arquivos de registro de comparecimento de eleitores e de registro digital do voto. Para isso, será necessário obter uma cópia dos arquivos antes e após um voto e, por meio da comparação entre a lista de comparecimento e da quantidade de votos dos candidatos saber qual foi o voto do eleitor.

2.2 – Fundamentação teórica

Não se aplica.

2.3 – Precondições para o teste

Atacante possui acesso físico a urna para romper o lacre abrir a urna antes e depois de um voto.

2.4 – Escopo – Superfície de ataque

Condições de operações e ambiente de votação.

2.5 – Janela de atuação simulada do atacante

Acesso a urna eletrônica durante a realização da eleição para retirada e cópia da memória de votação e/ou flash interna antes e depois de um voto. Acesso a urna eletrônica depois das eleições.

2.6 – Pontos de intervencão

Mídias de memória da urna eletrônica.

2.7 – Passos a serem realizados e material necessário

1. Atacante consegue acesso físico a urna depois de alguns votos registrados.
2. Atacante retira flash de votação e flash interna da urna eletrônica 10 min.
3. Atacante copia os arquivos de registro digital do voto e de comparecimento utilizando um computador e um adaptador de flash card compatível com a memória da urna. 10 min.
4. Atacante insere os cartões de memória de volta na urna. 5min.
5. Atacante espera o próximo voto.
6. Atacante retira novamente as memórias de votação. 10m.
7. Atacante copia os arquivos de registro digital do voto e de comparecimento. 5min.
8. Atacante aguarda o encerramento das eleições.
9. Utilizando as memórias geradas no passo 3, o atacante restaura o estado de memória da votação da urna ao instante do passo 2. 10 min.
10. Atacante encerra a votação na urna e obtém o Resultado 1. 5min.
11. Utilizando as memórias geradas no passo 7, o atacante restaura o estado de memória da votação da urna ao instante do passo 6. 10min.
12. Atacante encerra a votação na urna e obtém o Resultado 2. 5min.
13. Atacante compara Resultado 1 com o Resultado 2 e identifica o voto do eleitor. 5min.

Tempo de duração: 75 minutos.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

2.8 – Possíveis resultados e impacto

Com o ataque é possível quebrar o sigilo do voto de um eleitor. A extensão do ataque é 01 urna eletrônica.

2.9 – Rastreabilidade

O ataque só pode ser detectado no momento da retirada ou inserção da flash de votação na urna ou a percepção do rompimento dos lacres de segurança.

2.10 – Solução proposta

Para solucionar o possível ataque é necessário adotar uma memória flash card específica para a urna eletrônica na qual seja possível ler e escrever apenas por uma urna eletrônica. Deste modo, um atacante não conseguiria clonar a memória flash da urna.

RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

Individual – Marcelo Muzilli

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do plano de teste Invasão no transporte dos dados no sistema de votação		
Instituição proponente (se aplicável) **FindMee Assessoria Empresarial EIRELI ME**		
Responsável	Nome: Marcelo Muzilli *E-mail:* mmuzilli@findmee.com.br Telefone (do autor ou responsável): (11) 99850.5128	
Resumo do teste (máximo 120 caracteres)	O objetivo do teste é demonstrar somente um tipo de vulnerabilidade. Como exemplo, a vulnerabilidade de Inserção de SQL malicioso dentro da base de dados de votação poderá acarretar em graves problemas.	
Sistemas afetados	***Softwares*** ( ) *Software* de Gerenciamento de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE) ( ) *Software* Básico da Urna Eletrônica (X) *Software* de Carga (SCUE) ( ) *Software* Gerenciador de Aplicativos (GAP) ( ) *Software* de Votação (Vota) ( ) *Software* Recuperador de Dados (RED) ( ) Sistema de Apuração (SA) (X) Sistemas transportadores (X) *Kit JE Connect* (X) RecArquivos ( ) InfoArquivos ( ) Subsistema de Instalação e Segurança (SIS)	***Hardwares*** [ ] Urna eletrônica [ ] Mídias [ ] *Kit JE Connect* ***Procedimentos*** ( ) Geração de mídias ( ) Carga da urna ( ) Votação (X) Transmissão de arquivos
Duração estimada do teste (em minutos)	30	
Extensão do ataque	( ) Urna ou seção eleitoral ( ) Local de votação ( ) Zona eleitoral (X) Município (X) Unidade da Federação (X) País	
Conhecimentos necessários para a realização do teste	Segurança de Aplicação OWASP - https://www.owasp.org/index.php/Main_Page	

Observações:
- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá conter, no máximo, dez páginas em formato A4 ou Carta.

DETALHAMENTO DO TESTE

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

2.1 – Descrição geral do teste

O proponente deverá apresentar uma descrição geral do teste informado.

Conforme esquematizado nas Figuras 01 e 02, o teste consiste na exploração dos resultados na base de dados principal, onde fica concentrado o resultado de votação da nação. Esse resultado poderá ser adulterado com a inserção de scripts nocivos dentro do sistema.

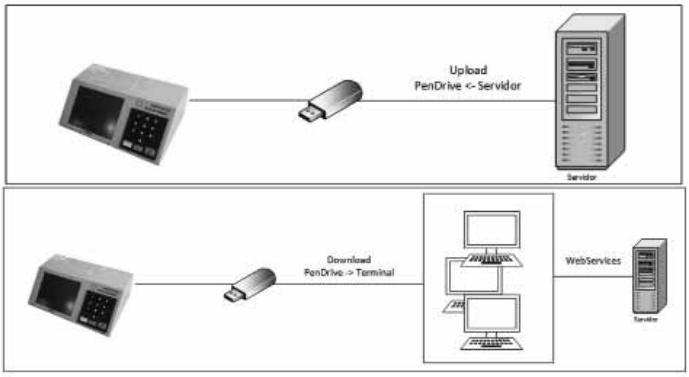


Figura: visto que o processo hoje ocorre manualmente, e com intervenção humana, a pessoa responsável poderá enviar o script nocivo para o servidor executar, e esse resultado poderá alterar o resultado para a Zona/Seção específica.
O objetivo do teste é demonstrar somente um tipo de vulnerabilidade. No exemplo, a vulnerabilidade de Inserção de SQL malicioso dentro da base de dados de votação poderá acarretar em graves problemas.
A transferência do resultado dos votos da zone eleitoral, hoje é feita de duas formas:

1. Forma manual (JE-Connect, linguagem Python).
2. Via consumo de serviço (Transportador, RecArquivos, linguagem Java)

Com um script pode-se modificar esse resultado alterando essas "tags" do cliente para interpretação do servidor. O servidor atualizará a base de dados com resultado adulterado no servidor.
Para demonstrar esse teste, exploraremos a seguinte vulnerabilidade conhecidas hoje:

1. SQL Injection [1]

Assim que o cliente executar o script responsável pelo envio dos dados para o servidor, pode-se alterar a tag SQL para a seguinte cláusula:

```
SELECT <Zona>, <Seção>, <Município>, <UF>, <CodCandidato>
  FROM TabelaDeVotacao
 WHERE <CodCandidato> = 'X';
       UPDATE <CodigoPartido>
       SET <CodigoPartido> = 1
       WHERE <CodCandidato> = 2';
```

Nesse script haverá a inclusão e modificação da tag SQL (exemplo demonstrado em vermelho) para ser modificado a tabela de votação.
Durante esse processo poderá ser feita a modificação do serviço no cliente que envia o resultado da zona eleitoral para o servidor. A adição de scripts maliciosos na aplicação que coleta esse resultado modifica-se ocultamente o processamento e resultado final dos votos.

2.2 – Fundamentação teórica

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

O teste procura mapear possíveis falhas durante o processo de transferência da mídia contendo os votos realizados na Zona Eleitoral para o Servidor onde irá totalizar os votos realizados no município e consequentemente ao estado e País.
Como esse processo hoje é realizado manualmente e com intervenção humana, um script malicioso poderá ser executado e no momento em que o Servidor consome esses dados, esse script poderá ofuscar, ou mascarar e alterar o conteúdo da mídia digital, alterando assim o resultado final da quantidade de votos.

2.3 – Precondições para o teste

Deverá ser apresentada lista contendo todas as informações e os recursos materiais (inclusive *software* e respectivas versões) e humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos-padrão de segurança adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto. Somente serão aceitos os relaxamentos solicitados cujo objetivo seja simular condições reais de cenários de ataque.

Para realização dos testes será necessária a utilização dos seguintes recursos:

a) 01 máquina (Cliente)
   a. A máquina em questão deverá ser a máquina cliente que irá ler o cartão de memória para envio ao servidor. Nessa máquina deverá ser instalado o aplicativo de invasão com 01 licença da ferramenta DAST PenTest para realizar o teste de penetração.
   b. ***Hardware mínimo (*).***
b) Acesso ao cliente e servidor.
   Entende-se como Cliente, a máquina que lê o cartão de memória e coleta as informações e Servidor entende-se como a máquina que envia a base de dados as informações contidas no cartão de memória.
c) URL da chamada do Serviço (Python ou Java).
d) Comunicação cliente <-> servidor sem bloqueador de acesso (Firewall)
e) Usuário de sistema responsável no acesso em disco (Leitura, Gravação e Exclusão)
f) Ferramenta automatizada de invasão ou PenTest (Teste de Penetração).
   a. Sugestão de Ferramenta DAST PenTest:
      i. HP WebInspect
g) Segmentação da rede: não é recomendável a utilização da ferramenta acima em ambiente de produção. Portanto, recomenda-se a utilização da mesma em ambiente pré-produção totalmente segmentado do ambiente produtivo; devido de a ferramenta ser invasiva no ambiente. Recomenda-se também o teste somente da aplicação. Este é um teste da aplicação e não do ambiente a ser testado.
h) Recurso Humano:
   a. Marcelo Muzilli – Formado em Tecnologia em Processamento de Dados, com 18 anos de experiência e 05 em Segurança de Dados e Aplicações

(*) Hardware Mínimo

	WebInspect Client	HP RTA
CPU	1.5GHz+ x 1	2GHz+
RAM	2GB+	2GB
HD	10GB	2GB
SO	Windows XP Pro+ Win Vista SP2 Windows 7 Windows 2003+	Windows Linux Redhat/Suse/Oracle EL Solaris 9/10 AIX
Banco de Dados	MS SQL Express 2008 R2	N/A
SW Adicional	MS .NET Framework 3.5 SP1+	Jboss/WebLogic/Websphere/Tomcat J9 (IBM) Oracle Java Hotspot Oracle Jrockit .NET 2.0, 3.0, 3.5, 4-0 IIS 5.1,6,7,7.5

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO

TSE

2.4 – Escopo – Superfície de ataque

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- material (ex.: urna, mídias, lacres, etc.);
- ambiente (ex.: condições de operação, sala, alimentação, etc.);
- procedimento (ex.: verificação, emissão de zerésima, etc.).

- Material: mídia eletrônica
- Procedimento: rodar ferramenta necessária para descoberta de possíveis brechas de segurança no Servidor e Processo JE-Connect.

2.5 – Janela de atuação simulada do atacante

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando-a com as precondições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

a) após o processo de votação ter-se concluído e,
b) transferência manual da mídia eletrônica para os servidores (JE-Connect e/ou Transportador).

2.6 – Pontos de intervenção

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *softwares* (ex.: programas assinados), *hardwares* (ex.: extensão proprietária de Bios), procedimentos (ex.: armazenamento de urnas), mídias (ex.: assinatura e criptografia do boletim de urna) e lacres.

A única intervenção será a existência de bloqueadores de acesso (Firewall ou WAFs) no servidor, do qual poderá impedir a tentativa de invasão no teste.

2.7 – Passos a serem realizados e material necessário

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim.

Os passos deverão ser detalhados e devem, obrigatoriamente, conter critérios de interrupção do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será do investigador.

Para realização dos testes será necessária a utilização dos seguintes recursos:

a) 01 máquina (Cliente)
   a. A máquina em questão deverá ser a máquina cliente que irá ler o cartão de memória para envio ao servidor. Nessa máquina deverá ser instalado o aplicativo de invasão com 01 licença da ferramenta DAST PenTest para realizar o teste de penetração.
   b. Hardware mínimo para instalação da solução no Apêndice I.
b) Acesso ao cliente e servidor.
   Entende-se como Cliente, a máquina que lê o cartão de memória e coleta as informações e Servidor entende-se como a máquina que envia a base de dados as informações contidas no cartão de memória.
c) URL da chamada do Serviço (Python ou Java).
d) Comunicação cliente <-> servidor sem bloqueador de acesso (Firewall)
e) Usuário de sistema responsável no acesso em disco (Leitura, Gravação e Exclusão)
f) Ferramenta automatizada de invasão ou PenTest (Teste de Penetração).
   a. Sugestão de Ferramenta DAST PenTest:
      I. HP WebInspect
g) Segmentação da rede: não é recomendável a utilização da ferramenta acima em ambiente de produção. Portanto, recomenda-se a utilização da mesma em ambiente pré-produção totalmente segmentado do ambiente produtivo; devido de a ferramenta ser invasiva no ambiente. Recomenda-se também o teste somente da aplicação. Este é um teste da aplicação e não do ambiente a ser testado.
h) Recurso Humano:
   a. Marcelo Muzilli – Formado em Tecnologia em Processamento de Dados, com 18 anos de experiência e 05 em Segurança de Dados e Aplicações

2.8 – Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. A descrição desses resultados deve conter:

- Tipo do resultado esperado. Ex.:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
  - [...].
- Extensão do ataque. Ex.:
  - urna ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.

O documento deverá ainda conter a probabilidade esperada de sucesso do ataque; se possível, fundamentada.

2.9 – Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, deve discorrer e fundamentar as condições e probabilidades de:

- não detectar o ataque;
- detectar o ataque.

Logo após a execução do software de descoberta de vulnerabilidade (DAST PenTest), gera-se um formulário com recomendações a serem executadas. É recomendado executar todos os procedimentos descritos.

2.10 – Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

Recomenda-se a utilização de ferramentas RASP (Runtime Application Self-Protection) de mercado como o produto HP RTA para bloqueio de tentativas de invasão e o monitoramento dessas invasões com ferramentas IAST (Interative Application Security Testing) da Contrast Security. Para a correção das vulnerabilidades em código fonte recomenda-se a utilização de ferramentas SAST (Static Application Security Testing) como HP Fortify e Checkmarx. Ambas, após o encontro das vulnerabilidades, recomenda-se auditar os códigos, e compila-los novamente.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

PROTOCOLO:

TSE

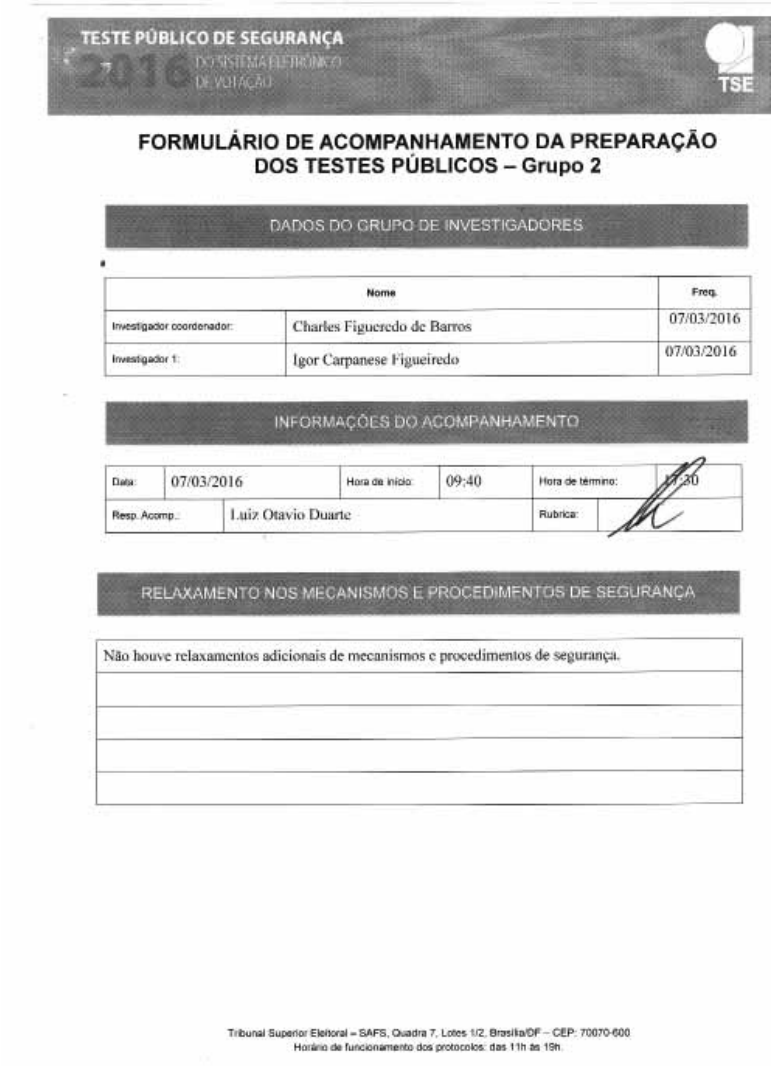
RESERVADO AO TRIBUNAL SUPERIOR ELEITORAL (TSE)

Protocolo	Data	
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado	

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – 70070-600 – Tel.: (61) 3030-7000
Protocolo Administrativo: sala V-101, fax: (61) 3030-9850 – Horário de funcionamento do protocolo: das 11h às 19h

Anexo E – Formulários de acompanhamento da preparação dos testes públicos

Grupo 2



TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

FORMULÁRIO DE ACOMPANHAMENTO DA PREPARAÇÃO DOS TESTES PÚBLICOS – Grupo 2

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	Charles Figueredo de Barros	07/03/2016
Investigador 1:	Igor Carpanese Figueiredo	07/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	07/03/2016	Hora de início:	09:40	Hora de término:	17:30
Resp. Acomp.:	Luiz Otavio Duarte			Rubrica:	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Não houve relaxamentos adicionais de mecanismos e procedimentos de segurança.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
	O presente documento tem por objetivo único relatar fatos importantes observados a partir do acompanhamento da preparação para os Testes Públicos de Segurança do Tribunal Superior Eleitoral de 2016.
	O investigador Sr. Charles Figueredo de Barros, coordenador do Grupo 2, chegou ao ambiente de preparação para os Testes Públicos de Segurança do Tribunal Superior Eleitoral de 2016 antes mesmo do horário convencionado de nove horas. Este aguardou pela chegada do Sr. Igor Carpanese Figueiredo, também membro de seu Grupo e pela liberação do ambiente de preparação.
09:40	Foi dado início ao processo de acompanhamento do Grupo 2. Este acompanhamento refere-se à preparação de ambiente realizada pelo Sr. Charles Figueredo de Barros – Coordenador do Grupo e pelo Sr. Igor Carpanese Figueiredo, para os Testes Públicos de Segurança 2016 do Tribunal Superior Eleitoral.
10:30	Após serem apresentados ao ambiente onde os trabalhos seriam realizados, foi liberado acesso ao computador CDE65 para o Sr. Igor Carpanese Figueiredo.
10:40	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, solicitou acesso ao hardware da Urna Eletrônica. Tendo sido questionado, o Sr. Cristiano Peçanha Correa, da comissão reguladora, liberou o acesso às urnas.
10:42	Os investigadores do Grupo 2 observaram o processo de boot (inicialização) da Urna Eletrônica. Ocorreu o entendimento do processo de boot e uso de mídias de carga, de votação e de mídias de resultados.
11:30	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, solicitou a criação de usuários nas máquinas CDE46 e CDE65 para os membros do Grupo 2, máquinas estas disponibilizadas para o Grupo 2, não sendo preenchidos formulários específicos para esta solicitação. Solicitação realizada ao Sr. Cristiano Peçanha Correa
11:40	Foram criados usuários nas máquinas para os membros do Grupo 2, Sr. Charles Figueredo de Barros e Sr. Igor Carpanese Figueiredo, em CDE46, através dos respectivos títulos eleitorais.
11:45	Foi criado usuário para o membro Sr. Charles Figueredo de Barros no sistema CDE65, através do número de seu título de eleitor.
11:50	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros e o Sr. Igor Carpanese Figueiredo, também membro do Grupo 2 observaram o sistema operacional da máquina CDE65 e o funcionamento do sistema GEDAI-UE.
12:00	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros gerou, mídia de carga para as seções já configuradas no Sistema GEDAI-UE através do software GEDAI-UE.
12:05	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros gerou, mídia de votação.
12:08	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros gerou, mídia de resultado.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

	Inicialmente foi gerada "mídia vazia" para verificar o que ocorreria se ela fosse inserida em uma das duas urnas pré-carregadas. - Observou-se que o sistema não inicia o sistema eleitoral se a "mídia vazia" for utilizada. - Com o sistema e com a mídia de "votação" (gerada em uma mídia de resultados), o sistema UE entrou em modo de votação.
12:20	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, iniciou um novo processo de carga finalizado.
12:30	Período de almoço. << nenhuma atividade realizada >>
14:00	Retorno dos investigadores e reinicio das atividades.
14:10	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, gerou **formulário** de requisição de software com: I – Pedido para provimento de instalação de ambiente de desenvolvimento. II – Pedido para o provimento de mídias de carga decifradas (sem o sistema de arquivos cifrado) III – Pedido para provimento de máquina com sistema operacional GNU/Linux.
14:20	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, pediu e foi prontamente atendido na solicitação para inspeção de códigos-fontes.
14:30	Alguns arquivos (ou classes) inspecionados: • cnomeeleitor • cpetitulo.cpp • ciniciovotação.cpp
15:00	A comissão reguladora apresentou resposta a solicitação formal de requisição de software com: I – Pedido para provimento de instalação de ambiente de desenvolvimento, será fornecido. II- Pedido para o provimento de mídias de carga decifradas (sem o sistema de arquivos cifrado), por ser uma barreira de segurança que devem ser transpostas, não serão fornecidas. III – Pedido para provimento de máquina com sistema operacional GNU/Linux, será fornecido.
15:23	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, preencheu **formulário** de pedido de informações: • Este formulário solicitava informações acerca do processo de liberação de eleitores. Especificamente informações sobre a iteração entre terminal de eleitor e Urna Eletrônica. • Comunicação entre threads e informações sobre o conceito de Ticks como mantenedores da sincronia entre as Threads.
15:40	Os membros do Grupo 2 realizam avaliação do arquivo cthreadeleitor.cpp

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

16:19	O responsável pela SEVIN, secretaria que desenvolve os sistemas de Urna Eletrônica, informa aos membros do Grupo 2 que o pedido de informações sobre o código-fonte não poderia ser atendido, pois não é objetivo dos testes explicar especificidades do código-fonte, ficando o entendimento a cargo do investigador.
16:30	Foi apresentado por representante da SEVIN as respostas aos questionamentos sobre as threads de mesário e urna, em alto nível. • O representante também reforçou que não é obtivo dos Testes Públicos de Segurança o escrutínio de códigos junto aos investigadores, mas sim dar os subsídios para que eles consigam fazer tal escrutínio por si só.
16:50	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, pediu um novo formulário para pedido dos arquivos de apresentação que foram feitas junto a etapa de disponibilização dos códigos-fonte.
17:15	Os investigadores finalizaram seu processo de inspeção códigos-fonte.
17:18	Os investigadores do Grupo 2 tiveram acesso aos documentos e apresentações realizadas no marco 5 e 6 dos Testes Públicos de Segurança. • Marco 5: "Palestra referente ao funcionamento tecnológico do sistema eletrônico de votação" • Marco 6: "Inspeção dos código–fonte"
17:20	Investigadores consultam documentos que tiveram acesso.
17:35	Investigadores do Grupo 2 terminam os trabalhos de preparação.
---	<< É o que havia a ser relatado. >>

Individual – João Felipe Souza

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — TSE

FORMULÁRIO DE ACOMPANHAMENTO DA PREPARAÇÃO DOS TESTES PÚBLICOS - Individual

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	João Felipe Souza	07/03

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	07/03/2016	Hora de início:	15:30	Hora de término:	17:46
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Não houve pedido de relaxamento nos mecanismos e procedimentos de segurança.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
	O presente documento tem por objetivo único relatar fatos importantes observados a partir do acompanhamento da preparação para os Testes Públicos de Segurança do Tribunal Superior Eleitoral de 2016.
15:30	Início de preparação dos testes.
15:40	Requisitado chave philips para abrir a Urna Eletrônica.
16:30	A Urna Eletrônica foi aberta.
16:52:	O investigador identificou a conexão USB que conecta o teclado da Urna Eletrônica com a placa mãe.
16:55	Foi solicitada permissão para pegar um cabo USB que o investigador trouxe, porém que está guardado fora da área do teste.
17:00	O Sr. Cristiano Peçanha, da Comissão Reguladora, aceitou a solicitação do investigador.
17:04	O investigador retira o conector do teclado da placa mãe; Conecta o teclado da urna no Adaptador USB de 2 portas; Na segunda porta do Adaptador USB conecta um cabo USB para um conversor USB/MicroUSB; Conecta o MicroUSB no Smartphone.
17:16	O investigador mantém o teclado da urna conectado no Adaptador USB; Conecta um cabo USB no computador.
17:28	O investigador conecta o Smartphone no computador; Realiza o teste para verificar se o teclado do Smartphone envia comandos para um editor de texto.
17:34	O investigador desconecta o teclado da urna da placa mãe; Conecta por meio do adaptador USB/MicroUSB o Smartphone na placa mãe; Liga a Urna; Preparação do Plano de teste finalizado.
17:46	Finaliza a preparação dos Testes.
---	<< É o que havia a ser relatado. >>
:	
:	
:	

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Anexo F – Formulários de acompanhamento dos testes públicos

Grupo 1

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Grupo 1

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	Sérgio Freitas da Silva	10/03/2016
Investigador 1:	André Henrique de Siqueira	Ausente

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	10/03/2016	Hora de início:	10:00	Hora de término:	17:30
Resp. Acomp.:	Antônio Theóphilo			Rubrica:	

DADOS DO TESTE

Título do teste:	Teste do sistema de apuração por votação totalmente eletrônica (digitar BU)	
Início do teste (data/hora):	10/03/2016	10:00
Término do teste (data/hora):	10/03/2016	17:30
Critério de parada:	Boletins de Urna (BU) forjados aceitos pelo Sistema de Apuração (SA)	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

O ataque exige a inutilização da Urna Eletrônica (UE), da mídia interna (MI), da mídia de votação (MV), da mídia de resultado (MR) e a posterior troca física do Boletim de Urna verdadeiro por um Boletim de Urna no momento de utilização do Sistema de Apuração (SA).

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
1	Simular uma votação na urna eletrônica e gerar um Boletim de Urna original.	Executado
2	Levantar os dados da votação, incluindo informações do pleito e do processo eleitoral.	Executado
3	Gerar e imprimir boletins de urna falsos.	Executado
4	Opcionalmente, pode-se apenas gerar os dados falsos do boletim de urna.	Executado
5	Digitar o Boletim de Urna falso, ou os dados falsos gerados, e verificar se são validados pelo Sistema de Apuração.	Executado

ACOMPANHAMENTO DOS FATOS

Hora	Fato
10:00	Chegada do investigador.
10:16	Conferência do material entregue ao investigador.
10:30	Explicação do teste a membros das Comissões Organizadora, Reguladora e Avaliadora.
10:40	Geração de mídia de carga.
10:50	Discussão sobre insumos.
11:00	Início de geração de BU autêntico.
12:20	Entrega de BU autêntico de Eleição Municipal (1º turno).
12:30	Realizada pausa para o almoço.
13:30	Retorno às atividades do período da tarde.
13:36	Solicitou ID do pleito, número do processo eleitoral, códigos dos cargos (via GEDAI-UE).
14:12	Solicitou um BU que contenha características específicas (votação apenas majoritária ou plebiscito) na versão Araticum.
14:50	A solicitação foi atendida.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

14:50	Carga gerada no GEDAI-UE.
14:55	Carga feita na Urna Eletrônica da votação e na Urna Eletrônica em que será executado o SA.
15:00	Início da votação (plebiscito)
15:20	Fim da votação, entrega do BU ao investigador.
15:20	Investigador iniciou sua análise do BU.
15:27	Investigador entrou no recinto reservado para ter mais privacidade e silêncio (acompanhado por um técnico do CTI) para poder gerar as colisões propostas.
16:22	Investigador retornou ao recinto de testes.
16:25	Iniciou-se o SA.
16:30	Solicitou-se uma pessoa para dar suporte de SA.
16:40	Iniciou-se a apresentação à Comissão Avaliadora.
16:45	Funcionário do TSE foi enviada para dar suporte à apresentação.
16:50	Iniciou-se a digitação do BU autêntico.
16:57	Interrompeu-se após a validação do código verificador.
16:58	Gerou-se um BU falso proposto pela Comissão Avaliadora.
16:59	O SA aceitou o código verificador.
17:00	O investigador informou que pode gerar BUs falsos que geram o mesmo código verificador mas com o pleito em questão não conseguiu (teste de colisões).
17:05	Iniciou-se a apresentação da falha no código-fonte para membros do Teste Público de Segurança.
17:30	Fim dos trabalhos.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O teste proposto foi alcançado com sucesso. O investigador tentou ampliá-lo gerando colisões de códigos verificadores de Boletins de Urna forjados mas não teve sucesso, segundo o investigador, devido a características do processo eleitoral utilizado no teste. O investigador solicitou para anexar a este formulário um relatório seu do plano de testes.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Nada a declarar.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR: _____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Grupo 2

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Grupo 02

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	Charles Figueredo de Barros	08/03/2016 e 09/03/2016
Investigador 1:	Igor Carpanese Figueiredo	08/03/2016 e 09/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	08/03/2016	Hora de início:	09:37	Hora de término:	16:24 do dia 09/03/2016
Resp. Acomp.:	Luiz Otavio Duarte			Rubrica:	

DADOS DO TESTE

Título do teste:	Ataque ao Sigilo do Voto	
Início do teste (data/hora):	08/03/2016	09:37
Término do teste (data/hora):	09/03/2016	16:24
Critério de parada:	Correlação de dados entre terminal do eleitor e terminal do mesário.	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Os investigadores devem poder instalar sistemas de software na Urna Eletrônica, em instante posterior à carga dos sistemas.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
1	Atacante identifica o protocolo de comunicação entre terminal do mesário e a urna.	Foram verificados os códigos-fonte do sistema.
2	Atacante tem acesso físico à Urna Eletrônica	Realizado com sucesso.
3	Atacante instala um software malicioso na urna, que ficará rodando em segundo plano durante a eleição.	Insucesso, ao identificar mecanismos de criptografia existentes.
4	Durante a eleição, o software captura as informações dos eleitores e seus respectivos votos.	---
5	Após a eleição, atacante tem acesso físico à urna e retira as informações armazenadas pelo software malicioso.	---

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 08/03/2016 >>
---	Durante o processo de preparação, os membros do Grupo 2 identificaram a existência de barreiras impostas por mecanismos de criptografia das mídias utilizadas nas Urnas Eletrônicas, o que levou o trabalho a se focar em formas de transpor tais barreira, além de aprofundar o conhecimento no processo de comunicação entre o terminal do mesário e a Urna Eletrônica.
9:37	Os investigadores, membros do Grupo 2, deram entrada no ambiente de testes de segurança.
9:40	Os investigadores, membros do Grupo 2, recebem máquina adicional com sistema GNU UBUNTU com o software Code:Blocks instalado.
9:56	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, preenche formulário requisitando esclarecimentos acerca de especificidades do termo de compromisso assinado pelos membros do Grupo 2.
10:16	O grupo realiza a inspeção de códigos-fonte.
11:55	Realizada pausa para o almoço.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

13:40	Retorno às atividades do período da tarde.
14:25	O grupo realiza inspeção de códigos-fonte. Segundo o coordenador do grupo o objetivo é identificar primitivas criptográficas utilizadas na cifração de dados das mídias, suas implementações, modo de operação, configuração e chaves. Esta é condição essencial para que o grupo consiga alterar dados das mídias para execução de seu plano de testes. A partir da inspeção dos códigos-fonte também é objetivo a identificação de pontos para proposição de novos testes.
16:43	O coordenador do Grupo 2, Sr. Charles Figueredo de Barros, preencheu novo formulário de pedido de informação técnica a cerca de que se declarações públicas sobre a Urna Eletrônicas e achados de código-fonte ferem o termo de confidencialidade:
---	<< É o que havia a ser relatado no acompanhamento do dia 08/03/2016 >>
---	<< Relato de acompanhamento de fatos relevantes do dia 09/03/2016 >>
14:30	Sem êxito, o coordenador do grupo de investigadores encerra os testes.
15:52	Visando dirimir eventual equivoco no entendimento sobre as informações solicitadas no seu último formulário de pedido de informação técnica (de 16:43 de 09/03) sobre os algoritmos, códigos-fonte e mecanismos utilizados na produção dos softwares de Urna, a comissão reguladora apresentou esclarecimentos sobre os pontos presentes no pedido. Dentre estes esclarecimentos, foram apresentadas incongruências entre o entendimento dos investigadores, exposto no pedido, e o que é de fato utilizado nos sistemas.
16:24	O representante da SEVIN, Sr. Rodrigo Coimbra, apresentou explicações sobre todos os pontos presentes no pedido original.
---	<< É o que havia a ser relatado no acompanhamento do dia 09/03/2016 >>

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O plano de teste proposto pelo grupo de investigadores pressupunha a alteração de executáveis das Urnas Eletrônicas. Entretanto, o grupo não obteve êxito no processo de decifração e alteração de dados das mídias.

Faz-se importante relatar que houve dificuldade do grupo de investigadores no entendimento dos códigos-fonte dos sistemas de software de Urna Eletrônica, em parte pelo grande número de linhas de códigos, em parte pela restrição de tempo e em partes pelo não acompanhamento do grupo de investigadores do evento de apresentação dos sistemas e códigos-fonte. Tal evento dos testes públicos ocorreu em momento anterior às etapas de preparação e testes.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

A execução do plano de testes foi prejudicada, em parte, pela impossibilidade de comparecer aos eventos anteriores ao TPS (palestra de apresentação e inspeção dos códigos-fonte, realizadas em janeiro), nos quais foram apresentadas explicações a respeito do funcionamento do sistema de votação. Esta impossibilidade foi causada pela janela de tempo entre os eventos. Além disso, problemas técnicos impossibilitaram o acesso prévio aos arquivos disponibilizados pelo TSE, arquivos estes que continham as explicações apresentadas na palestra do dia 11 de janeiro e incluíam o vídeo da referida palestra. Sugere-se a diminuição desta janela temporal entre os eventos, facilitando a participação em todos eles, sobretudo para residentes de outras cidades ou estados, ou a realização dos eventos prévios (palestras de apresentação do sistema e inspeção do código-fonte) localmente, nos respectivos TRE's.

Durante a fase de preparação, deparamos com um obstáculo à execução do plano de testes, que foi o fato das mídias de carga serem cifradas. Fizemos um requerimento para que fossem disponibilizadas mídias decifradas, mas este foi indeferido. Acreditamos que o acesso a mídias decifradas simula, de forma realista, um cenário de ataque perpetrado por agentes internos com acesso privilegiado, embora seja válido ressaltar que a cifração das mídias constitui uma barreira de segurança contra agentes externos.

Ressaltamos e reconhecemos avanços positivos, como a diminuição nas restrições de acesso ao código-fonte, a prontidão da comissão reguladora em responder aos questionamentos apresentados e a possibilidade de proposta de novos planos de teste mesmo durante a execução do TPS.

Elogiamos a iniciativa do TSE em realizar os Testes Públicos de Segurança. Ao mesmo tempo, ressaltamos que a publicidade deste evento deve ser voltada para a afirmação de que o objetivo do teste é avaliar a segurança e os riscos envolvidos na utilização da urna eletrônica, e não simplesmente confirmar que a mesma é segura.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR:

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Grupo 4

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Grupo 4

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	Elisabete Evaldt	08 a 10/03/2016
Investigador 1:	Gustavo Henrique Cervi	08 a 10/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	08/03/2016	Hora de início:	11:00	Hora de término:	15:30
Resp. Acomp.:	Edmar Roberto Santana de Rezende			Rubrica:	

DADOS DO TESTE

Título do teste:	Tentativa de fraude na destinação dos votos.	
Início do teste (data/hora):	08/03/2016	11:00
Término do teste (data/hora):	10/03/2016	15:30
Critério de parada:	Conseguir alterar a destinação do voto através de controle dos dispositivos de teclado e impressora explorando uma modificação na mídia de carga.	

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Não houve.

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	Status
1	Atacante tem acesso à mídia de carga da urna, após ser gerada e antes de ser utilizada na urna eletrônica.	Executado
2	Utilizando um computador portátil, lê a mídia de carga no intuito de violar o sigilo das partições de arquivos.	Executado
3	Atacante recupera arquivos do sistema operacional da urna e substitui partes de suas instruções.	Executado
4	A mídia deverá ser usada normalmente para carregamento da urna pelo TSE sem acusar a violação.	Executado

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 08/03/2016 >>
11:00	Foram apresentados os recursos computacionais ao grupo.
11:05	Realizada a conferência dos equipamentos entregues.
11:10	Grupo dirigiu-se ao ambiente de inspeção de código-fonte.
11:11	Grupo realizou uma análise preliminar do código-fonte buscando se familiarizar com o conteúdo e organização do mesmo.
12:00	Grupo deixou o ambiente de inspeção de código-fonte.
12:03	Análise do pôster "Visão Sistêmica do Processo Eleitoral (2016)".
14:25	Foi preenchido um Formulário de Requisição de Material solicitando um computador com sistema operacional UBUNTU instalado e um multímetro.
14:35	Grupo utilizou o sistema GEDAI-UE para gerar uma mídia de carga para a Seção Eleitoral 28.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

14:40	Grupo montou a mídia de carga utilizando um sistema Ubuntu Linux e criou um arquivo na segunda partição (onde encontra-se o *kernel* cifrado do UENUX).
14:45	Grupo realizou a carga da urna com a mídia de carga modificada com sucesso. Nenhuma mensagem de erro foi emitida durante a carga.
14:50	Grupo montou a mídia de carga novamente e criou um arquivo na terceira partição.
14:55	Grupo tentou realizar a carga da urna sem sucesso. Uma mensagem de erro foi emitida durante o processo de *boot* da urna com a mídia de carga modificada.
15:00	Grupo montou a mídia de carga, apagou o arquivo */dev/lp0* existente na terceira partição e criou um link */dev/lp0* apontado para */dev/video0*, com o intuito de verificar se a impressão seria desabilitada.
15:05	Grupo inseriu a mídia de carga modificada na urna e reimprimiu o Extrato de Carga da última carga válida realizada. Nenhuma mensagem de erro foi emitida durante a carga.
15:10	Grupo utilizou o sistema GEDAI-UE para gerar uma mídia de carga para a Seção 29.
15:20	Grupo modificou arquivos na terceira partição da mídia de carga, apagando todos os arquivos */dev/lp0-255* e criando links desses arquivos para */dev/video0*.
15:25	Grupo realizou a carga da urna utilizando a mídia modificada, no entanto esperava-se que o Extrato de Carga não fosse impresso, o que não ocorreu como esperado.
15:30	O computador com sistema UBUNTU Linux instalado e o multímetro foram entregues ao grupo.
15:35	Grupo preencheu Formulário de Requisição de Material solicitando um conector USB extra para mídias de carga.
15:40	Grupo modificou arquivos na terceira partição da mídia de carga, apagando todos os arquivos */dev/ueprt0-255* e criando links desses arquivos para */dev/video0*.
15:45	Grupo realizou a carga da urna utilizando a mídia modificada, no entanto esperava-se que o Extrato de Carga não fosse impresso, o que não ocorreu como esperado.
17:29	O conector USB extra solicitado foi entregue ao grupo.
---	<< Relato de acompanhamento de fatos relevantes do dia 09/03/2016 >>
10:30	Grupo, em parceria com integrantes do Grupo 5, montaram a mídia de carga e realizaram a análise de *dumps* das partições utilizando os comandos *hexdump* e *strings*, com o intuito de decodificar informações que possam eventualmente ser alteradas, visando burlar os mecanismos de verificação de integridade existentes no sistema.
11:00	Grupo dirigiu-se ao ambiente de inspeção de código-fonte.
11:01	Grupo realizou uma análise do código-fonte buscando por comentários e/ou código que pudesse auxiliá-los no entendimento do sistema.
12:00	Grupo deixou o ambiente de inspeção de código-fonte.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

14:00	Grupo, em parceria com o Investigador João Felipe Souza, iniciou análise do hardware da urna com o objetivo de identificar possíveis comunicações internas entre os dispositivos que pudessem ser interceptados.
14:40	Grupo realizou alterações nos *dumps* da mídia de carga, alterando *strings* existentes na primeira partição (FAT12) e sobrescreveu a partição da mídia de carga com as informações modificadas.
14:45	Grupo iniciou os testes de carga da urna com a mídia modificada e o *boot* foi realizado com sucesso. No entanto, verificou-se que as alterações não surtiram o efeito desejado.
15:06	Grupo preencheu Formulário de Requisição de Material solicitando o *datasheet* do hardware da urna e da impressora.
17:20	O *datasheet* da impressora foi entregue ao grupo, no entanto as informações desejadas pelo grupo não estavam presentes no documento entregue.
17:30	O Sr. Rafael, da Comissão Reguladora, esclareceu todas as dúvidas dos integrantes do grupo sobre detalhes do hardware da urna e da impressora.
---	<< Relato de acompanhamento de fatos relevantes do dia 10/03/2016 >>
11:00	Grupo dirigiu-se ao ambiente de inspeção de código-fonte.
11:01	Grupo realizou uma análise do código-fonte buscando por comentários e/ou código que pudesse auxiliá-los no entendimento do sistema.
11:30	Grupo deixou o ambiente de inspeção de código-fonte.
11:35	Grupo e o investigador João Felipe discutiram técnicas e estratégias para análise das mídias eleitorais no sistema Linux.
15:00	Grupo realizou um debate final com o responsável pelo acompanhamento apontando e discutindo detalhadamente as estratégias utilizadas durante o Teste Público de Segurança para viabilizar o Plano de Testes proposto e relatando ideias que surgiram durante o evento.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O Plano de Testes proposto pelo Grupo 4 (composto pelos investigadores Elisabete Evaldt e Gustavo Henrique Cervi) foi executado integralmente, contudo não alcançou os resultados esperados.

O Grupo realizou diversas análises do código-fonte dos sistemas GEDAI-UE e UENUX com o objetivo de entender melhor o funcionamento dos sistemas e identificar possíveis pontos de vulnerabilidade, no entanto nenhuma fragilidade foi identificada.

O Grupo também realizou diversas análises da mídia de carga com o objetivo de avaliar se seria possível realizar alterações no conteúdo da mídia que modificassem o comportamento do sistema sem serem identificadas pelos mecanismos de checagem de integridade existentes, no entanto os testes realizados não alcançaram os resultados esperados.

Além disso, o Grupo interagiu bastante com os demais grupos buscando identificar possíveis estratégias alternativas para alterar a destinação do voto através da interceptação da comunicação dos dispositivos de hardware internos da urna, no entanto nenhuma nova abordagem foi proposta.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Em termos gerais, o grupo ficou consideravelmente satisfeito com o evento e o teste realizado nos equipamentos e códigos-fonte disponibilizados para a investigação. A equipe do TSE foi cooperativa e atendeu com razoável prontidão as nossas solicitações de equipamentos e informações. Do ponto de vista técnico foi possível confirmar a segurança dos dispositivos e parte do sistema que foi alvo do nosso teste. Gostaríamos, no entanto, de sugerir pontos de melhoria para as próximas edições: a) O ambiente foi demasiadamente turbulento, atrapalhando um pouco a concentração que o exercício científico exige, sendo assim, recomendamos o isolamento por meio de parede de vidro dos profissionais de imprensa e outros participantes. b) O acesso às informações poderia ser através dos profissionais que trabalham no projeto, auxiliando na pesquisa e testes, trabalhando em caráter de cooperação. Entendemos que não há tempo hábil para inferir toda a extensa documentação, portanto o apoio de um profissional com profundos conhecimentos - para apenas consultas - seria de grande valia para a realização de experimentos. c) O acesso a documentação pessoal do investigador poderia ser flexibilizado permitindo a entrada de equipamentos pessoais limitados como e-readers ou tablets, desde que não permitam a cópia de informações e captura de áudio e imagens - o que é perfeitamente compreensível e louvável.
Por fim, reforçamos a nossa satisfação com o que vimos, seria uma falácia científica de nossa parte garantir que o sistema é 100% seguro, mas podemos dizer com relativa tranquilidade que a solução é de altíssimo nível tecnológico e conta com poderosos recursos anti-fraude.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR: _____

_____
ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Grupo 5

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Grupo 5

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	Luis Fernando de Almeida	08 a 10/03/2016
Investigador 1:	Jeferson Lesbão de Siqueira	08 a 10/03/2016
Investigador 2:	Alison Luiz de Oliveira Chaves	08 a 10/03/2016
Investigador 3:	Vinicius Zibetti Resko	08 a 10/03/2016
Investigador 4:	Fabio Rosindo Daher de Barros	08 a 10/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	08/03/2016	Hora de início:	10:20	Hora de término:	16:30 do dia 09/03/2016
Resp. Acomp.:	Guilherme Cesar Soares Ruppert			Rubrica:	

DADOS DO TESTE

Título do teste:	Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual.	
Início do teste (data/hora):	08/03/2016	10:20
Término do teste (data/hora):	09/03/2016	16:30
Critério de parada:	Quando o áudio for transmitido para outro computador.	

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Mesário deve digitar o código de habilitação manual do áudio.

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
1	Acesso à Urna Eletrônica.	Executado.
2	Acoplar de dispositivo à saída de áudio.	Executado.
3	Iniciar votação.	Executado.
4	Mesário habilita o áudio.	Executado.
5	Dispositivo captura e envia o áudio.	Executado.

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 08/03/2016 >>
10:20	Chegada dos investigadores.
10:30	Conferência dos materiais que serão utilizados no teste.
11:00	Início do processo de geração das mídias.
11:10	Início do processo de Carga da Urna Eletrônica.
11:40	Realizada requisição de materiais: Cabos ethernet, switch, computador com sistema operacional GNU/Linux e monitor.
12:04	Pausa para o período de almoço.
14:15	Retorno do período do almoço e reinício das atividades.
14:26	Urna Eletrônica colocada em processo de votação.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

14:28	Responsável pela SEVIN, Sr. Rodrigo Coimbra, informou ao grupo de investigadores que o audio pode ser habilitado manualmente pelo mesário através do código 888888888888.
14:30	Grupo simulou uma votação e conseguiu ouvir o áudio no fone de ouvido após liberar o áudio manualmente.
15:00	Grupo prepara um dispositivo portátil (RaspberryPi – que executa o serviço IceCast) que possui uma interface de áudio para conectar à saída de áudio da Urna Eletrônica e transmitir o áudio para outro computador via rede ethernet.
15:55	Grupo conseguiu efetuar o envio do áudio para outro computador através da rede ethernet. Como o dispositivo possui interface do tipo WiFi, a transmissão sem fio seria facilmente bem sucedida. Foi necessária a liberação manual do áudio.
16:30	O Grupo encerrou as atividades do dia.
--	<< É o que havia a ser relatado das atividades do dia 08/03/2016>>
---	<< Relato de acompanhamento de fatos relevantes do dia 09/03/2016 >>
09:30	O Grupo de investigadores inicia o fechamento dos testes, desenvolvendo o relato dos investigadores.
---	<< Teste concluído e encerrado >>

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O grupo obteve sucesso no ataque, conseguindo transmitir o áudio do voto para os seguintes casos:

1. Urnas que possuem o áudio habilitado para todos os eleitores por padrão (locais com grande quantidade de eleitores com deficiência visual);
2. Votos de pessoas com deficiência visual;
3. Votos habilitados manualmente pelo mesário mediante decisão própria (assumindo envolvimento malicioso deste) ou por solicitação do eleitor.

Adicionalmente, é importante observar que a traseira da Urna Eletrônica, onde a saída de áudio fica localizada, está visível todo o tempo para os mesários, eleitores e fiscais, o que poderia facilitar a identificação de dispositivos estranhos conectados.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Este relatório tem por objetivo apresentar informações as quais o grupo considera pertinentes e relevantes para entendimento do ataque proposto do plano de teste apresentado no TESTE PÚBLICO DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO promovido pelo Tribunal Superior Eleitoral (TSE).

De forma preliminar, constata-se que o constante avanço tecnológico proporciona, dentre outras coisas, uma tendência de modularização e miniaturização de diversos dispositivos. Entretanto, observa-se que isso não tem comprometido a sua capacidade de atuação, a sua aplicabilidade e o seu processamento, dentre outros aspectos. Pelo contrário, verifica-se, inclusive, o aumento do potencial de sua atuação e, adicionalmente, a possibilidade de inclusão de novas funcionalidades.

Diante desse contexto, dispositivos de dimensões reduzidas podem ser utilizados para ataques aos mais diversos sistemas de segurança, incluindo aqui, o sistema eleitoral brasileiro e, mais especificamente, a urna eletrônica.

No ataque proposto e apresentado no plano de teste, propõe-se a utilização de um dispositivo, como por exemplo, do tipo Raspberry PI, capaz de capturar o áudio referente ao voto de um eleitor e transmiti-lo para outros dispositivos nas proximidades, ou mesmo distantes via internet, utilizando uma rede, por exemplo, do tipo wifi.

A motivação do ataque, além do exposto referente ao avanço tecnológico, está condicionada a existência de um cenário previsível e factível o qual engloba, principalmente, duas particularidades:

a) a configuração da urna com relação à habilitação de áudio;

b) o modo no qual o acoplamento do dispositivo será executado na urna eletrônica a fim de habilitar a transmissão do áudio referente ao voto do eleitor.

Com relação ao primeiro item, o cenário para a eficácia do ataque está condicionado aos seguintes casos:

- urnas eletrônicas cujo áudio está previamente habilitado para todo o processo de votação, ou seja, para todo eleitor;
- urnas que apresentam o áudio habilitado somente alguns eleitores previamente cadastrados, devido a alguma deficiência visual;
- urnas as quais a habilitação do áudio está condicionada a ação manual do mesário pela digitação do código "8888888888" mediante decisão própria ou solicitação do eleitor.

Para o segundo item, podem ser consideradas as seguintes opções:

a) o dispositivo pode ser acoplado na urna antes de iniciar o processo de votação;

b) o dispositivo pode ser acoplado na urna durante o processo de votação no momento que um eleitor necessite a utilização do áudio para o seu voto ou pela ação voluntária e maliciosa de algum componente da seção eleitoral;

c) o dispositivo pode ser acoplado na urna de modo temporário, somente durante o voto de um determinado eleitor. Nesse caso, o eleitor o carrega consigo no bolso, por exemplo, o dispositivo de transmissão de dados e entrega para o mesário o plug conectado a esse dispositivo, induzindo a acreditar ser proveniente do fone de ouvido.

Tendo em vista a existência de uma das condições dos cenários descritos anteriormente, o processo para quebra de sigilo do voto se daria da seguinte forma:

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

- o eleitor se dirige à urna eletrônica para realização para exercício de seu direito de voto;
- durante o processo de sua votação, o dispositivo acoplado à urna eletrônica recebe todo áudio, mediante uma das opções apresentadas anteriormente, referente ao voto desse eleitor e transmite, por meio de uma rede wifi, por exemplo, para quaisquer dispositivos na proximidades da seção eleitoral fazendo com que o voto desse eleitor possa ser ouvido por outros dispositivos (celulares, computadores, tablets, etc.) A quebra do sigilo do voto seria concretizada mediante a existência de uma pessoa, presente na seção eleitoral que sofre o ataque, registrando a sequência dos eleitores que estão votando. Com isso, concretizaria a quebra do sigilo do voto com a associação/mapeamento do áudio executado com o eleitor que efetuou o voto.

De uma forma mais ampla do ataque, poderia-se pensar em um sistema disponibilizado de forma *online* na internet. Nesse contexto, teria-se uma rede configurada para a transmissão do áudio via internet. Ao mesmo tempo, a pessoa presente na seção sofrendo o ataque poderia ter um aplicativo para dispositivo móvel o qual ele, também de forma *online*, disponibilizaria os dados referentes à sequência de eleitores que estão votando. Com isso, teria-se a possibilidade de quebra de sigilo de âmbito aberto a todos que se interessassem em saber em quem cada eleitor está votando na seção em ataque. Um ponto importante sobre a quebra do sigilo do voto de um eleitor é o fato desse ataque ser direcionado a uma seção com a presença de pessoas públicas importantes, o qual a quebra do sigilo poderia acarretar em consequências mais críticas.

Como alternativas e propostas de ações corretivas para o problema detectado sugere-se:

- Uma ação mais eficiente e eficaz seria a inclusão de criptografia no processo de geração do áudio e consequente utilização de um fone de ouvido específico o qual impossibilitaria a captação e transmissão do voto capturado pelo dispositivo de áudio.
- Devido a possibilidade de inviabilidade econômica e/ou temporal para execução da ação corretiva anterior, uma alternativa seria o acoplamento à saída de áudio de um extensor fixo, não removível. Assim, o conector para o fone de ouvido estaria sempre visível inviabilizando a ação de acoplamento de dispositivo de forma oculta.
- Alteração do Manual do Mesário, incluindo a inspeção visual da parte traseira da urna eletrônica, comparando-a com uma foto padrão impressa no respectivo manual. Sugere-se que essa inspeção seja efetuada antes do início da eleição e tenha, obrigatoriamente, a participação de todos os componentes da seção e de possíveis testemunhas adicionais (primeiros eleitores, fiscais de partidos, por exemplo), assinando-se um documento para registro da inspeção.
- Alteração do Manual do Mesário, incluindo procedimento para execução do voto utilizando o áudio. Nesse caso, sugere-se que o fone de ouvido, obrigatoriamente, seja apresentado ao mesário e esse faça conexão para, depois início do voto.
- Alteração na tela de visualização da urna de tal forma que, toda a vez que o áudio seja habilitado, exiba-se uma mensagem, em forma de texto, informando a ativação do áudio, possibilitando ao eleitor questionar o fato, visto que ele não o tenha solicitado.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR: _____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Individual – João Felipe Souza

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Individual – Destruidor de Votos

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	João Felipe Souza	09/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	09/03/2016	Hora de início:	14:23	Hora de término:	15:46
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

DADOS DO TESTE

Título do teste:	Destruidor de Votos.	
Início do teste (data/hora):	09/03/2016	14:23
Término do teste (data/hora):	09/03/2016	15:46
Critério de parada:	Quando conseguir computar somente o eleitor e não o voto.	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Não houve pedido de relaxamento nos mecanismos e procedimentos de segurança.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
	Teste I	
1	Atacante insere dispositivo eletrônico radiocontrolado na bateria interna da urna	Executado.
2	Atacante prepara ambiente e interrompe o fornecimento de energia elétrica da seção.	O investigador não trouxe o dispositivo eletrônico, o teste foi realizado de forma manual, onde o investigador interrompeu o fornecimento de energia manualmente direto na bateria da Urna Eletrônica com o cabo de energia elétrica desligado da tomada.
3	Atacante acessa a cabina de votação para votar.	Executado.
4	Atacante aciona mecanismo para desligar a urna no momento da gravação do seu voto.	Executado.
5	Urna registra o comparecimento, mas não registra o voto, o teste foi bem sucedido.	Não obteve resultado positivo.
6	Atacante obtém acesso a urna depois das eleições para remover mecanismo radiocontrolado.	---

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

. TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 09/03/2016 >>
14:23	Investigador inicia o teste.
14:30	Insere a Mídia de Carga na Urna Eletrônica.
14:33	Liga a Urna Eletrônica e configura para simulação de eleição.
14:38	Troca a Mídia de Carga por Mídia de Votação.
14:39	Insere a Mídia de Resultados
14:45	Segue os procedimentos de checagem da Urna Eletrônica (teclado, impressora e vídeo).
14:53	Início da votação com a Urna Eletrônica sem alimentação de energia (somente bateria).
14:56	Votação do eleitor 1.
14:58	Votação do eleitor 2.
15:00	Votação do eleitor 3 com interrupção de energia antes de apertar a tecla "Confirma" (desligamento da Urna Eletrônica).
15:01	A Urna Eletrônica foi religada. Ao iniciar apareceu na tela a mensagem para inserir o código de reinício. O código foi inserido na Urna Eletrônica.
15:02	Verificou-se que título do eleitor 3 não foi computado.
15:13	O teste com o eleitor 3 com o desligamento da urna antes de apertar a tecla "Confirma" foi realizado novamente. Verificou-se que o título de eleitor foi computado.
15:15	O mesmo teste foi realizado com o eleitor 4 onde o título de eleitor também foi computado.
15:22	O mesmo teste foi realizado com o eleitor de número 5, e verificado que o título de eleitor também foi computado.
15:25	O teste foi realizado novamente com o eleitor 6 e o título de eleitor não foi computado na Urna Eletrônica.
15:30	Mais dois votos foram realizados sem o desligamento da Urna Eletrônica e computados normalmente.
15:40	A simulação da eleição foi finalizada e impresso o BU para conferência.
15:45	Resultado do BU gerado foi de 7 eleitores com 7 votos computados.
15:46	Sem êxito, o investigador encerra os testes.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

. TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

---	<< É o que havia a ser relatado >>

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O teste envolve o corte da energia elétrica e da bateria durante a votação de um eleitor. A ideia é que no momento da confirmação do voto, o corte da energia ocorra e ocorra o desligamento Urna Eletrônica. Com isso, espera-se que o voto não seja computado, porém que o eleitor seja registrado normalmente.

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Nada a declarar.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR: _____

_____
ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Individual – Registrador do Teclado

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	João Felipe Souza	08/03

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	08/03/2016	Hora de início:	11:40	Hora de término:	16:40
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

DADOS DO TESTE

Título do teste:	Registrador do teclado	
Início do teste (data/hora):	08/03/2016	11:40
Término do teste (data/hora):	08/03/2016	16:40
Critério de parada:	Quando conseguir capturar o voto.	
	Quando conseguir digitar o voto.	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Não houve pedido de relaxamento nos mecanismos e procedimentos de segurança.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
	Teste I	
1	Atacante tem acesso físico a urna eletrônica antes das eleições.	Executado.
2	Atacante viola os lacres de segurança.	Não havia lacres.
3	Atacante abre a urna eletrônica.	Executado.
4	Atacante introduz o dispositivo eletrônico para registro do teclado	Foi conectado o dispositivo com sucesso. A Urna Eletrônica foi reiniciada, entretanto interrompeu sua inicialização, pois reconheceu um hardware não validado.
5	Atacante fecha a urna.	---
6	Atacante reposiciona os lacres de segurança.	---
7	Durante as eleições o atacante registra a ordem de votação dos eleitores.	---
8	Atacante obtém acesso a urna eletrônica após a realização das eleições.	---
9	Atacante realiza a retirada do dispositivo eletrônico de registro do teclado e obtém sequência de votação.	---
	Teste II	
1	Atacante tem acesso físico a urna eletrônica antes das eleições.	Executado.
2	Atacante viola os lacres de segurança	Não havia lacres.
3	Atacante abre a urna eletrônica.	Executado.
4	Atacante substitui teclado original por outro teclado USB.	O computador não conseguiu ler dados do *device descriptor* do teclado tão pouco as teclas digitadas no teclado da Urna Eletrônica.

TE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

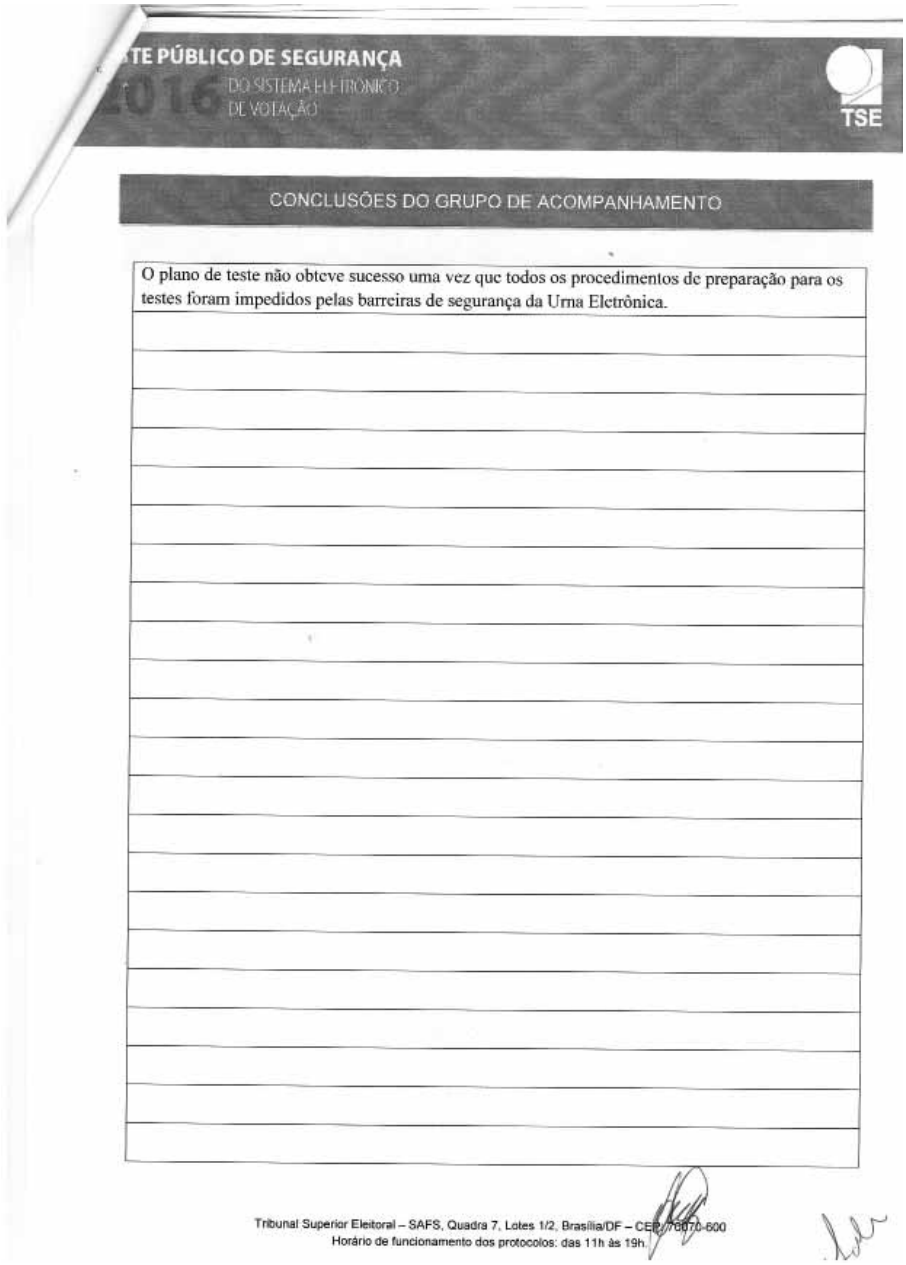
5	Atacante fecha a urna.	---
6	Atacante reposiciona os lacres de segurança.	---
7	Durante as eleições o atacante registra a ordem de votação dos eleitores.	---
8	Atacante obtém acesso a urna eletrônica após a realização das eleições.	---
9	Atacante realiza a retirada do dispositivo eletrônico de registro do teclado e obtém sequência de votação.	---
	Teste III	
1	Atacante tem acesso físico a urna eletrônica antes das eleições.	Executado.
2	Atacante viola os lacres de segurança.	Não havia lacres.
3	Atacante abre a urna eletrônica.	O computador não conseguiu ler dados do *device descriptor* do teclado tão pouco as teclas digitadas no teclado da Urna Eletrônica.
4	Atacante conecta o teclado da urna no computador via porta USB para obter padrões a parâmetros de configuração do teclado virtual.	---
5	Atacante substitui teclado original por uma conexão USB com a máquina para conexão do teclado virtual, hipoteticamente seria um teclado fisicamente idêntico ao teclado original da urna.	---
6	Atacante fecha a urna.	---
7	Atacante inicia a urna eletrônica e, caso seja iniciado normalmente o teste será bem sucedido.	---

DE VOTAÇÃO

TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 08/03/2016 >>
11:42	Investigador inicia o teste.
11:44	O investigador liga a Urna Eletrônica para a verificação de integridade do sistema.
11:47	Realiza a abertura da Urna Eletrônica e desconecta a USB do teclado do eleitor da placa mãe.
11:51	Conecta a USB do teclado da Urna Eletrônica no HUB USB.
11:52	Conecta o cabo USB no HUB USB e no SmatPhone utilizando um adaptar USB/MicroUSB.
11:54	Configura e testa o SmatPhone conectado com a Urna Eletrônica.
12:18	O SmartPhone reconheceu a conexão com a Urna Eletrônica, porém não reconheceu as teclas digitadas da Urna Eletrônica.
12:25	O investigador conecta o SmartPhone dircto na placa mãe da Urna Eletrônica.
12:27	Liga aUrna Eletrônica
12:30	Com o SmartPhone conectado na Urna Eletrônica aparece a mensagem: "ST13runtime-Error" CinputKbd-Create Instance -Falha ao conectar o SCR.
12:32	Investigador testa a Urna Eletrônica ligando-a sem nenhum teclado conectado para verificar a repetição do erro.
12:34	O erro se repete.
12:45	Pausa para o período de almoço.
13:43	Retorno do período do almoço e reinicio das atividades.
14:02	Investigador conecta o teclado da Urna Eletrônica no computador com o sistema operacional GNU UBUNTU para testar os dígitos.
14:33	Investigador gera Flash de Carga e Votação.
14:55	Teste com SmartPhone conectado ao computador.
15:20	Teste com teclado da Urna Eletrônica.
16:40	Sem êxito, o investigador encerra os testes.
---	<< É o que havia a ser relatado >>

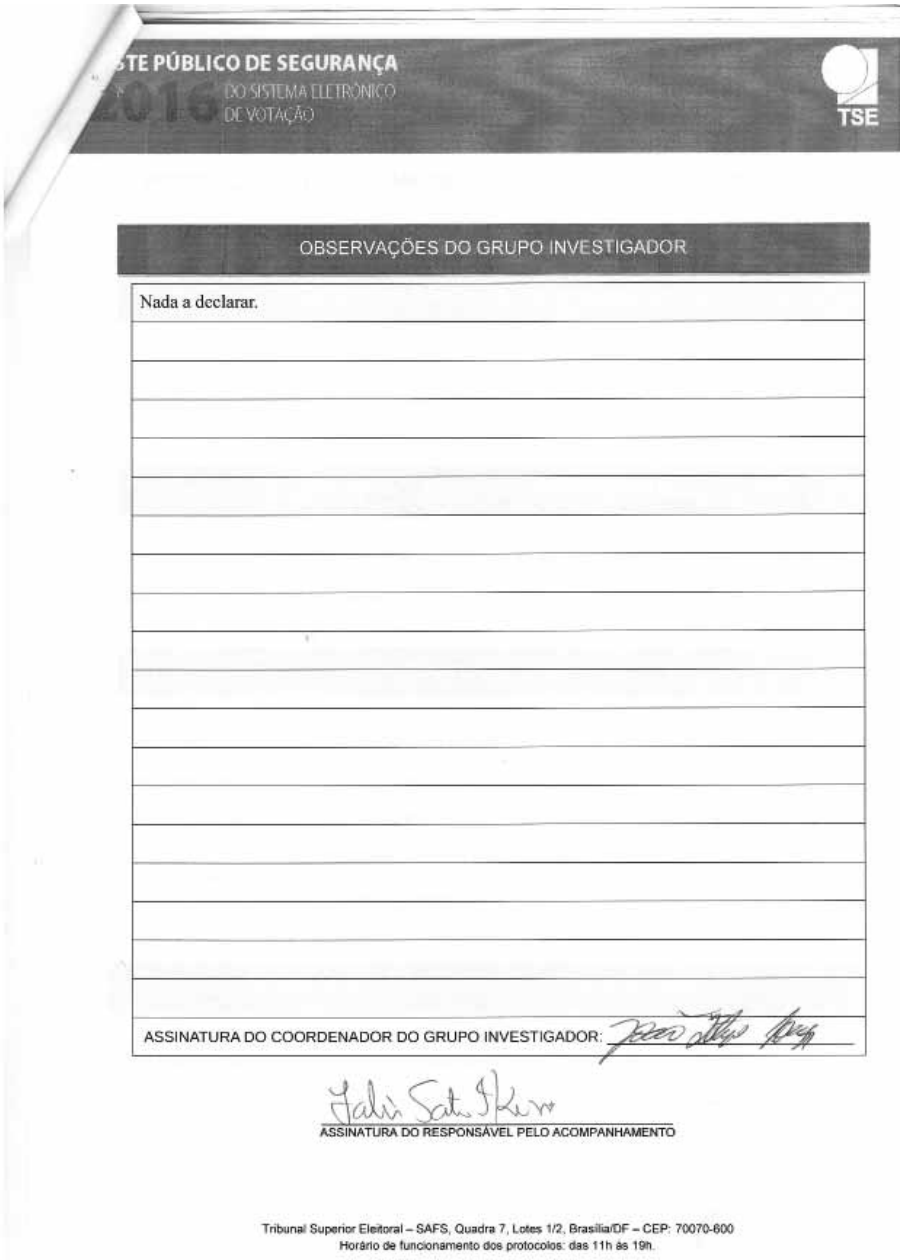


TE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O plano de teste não obteve sucesso uma vez que todos os procedimentos de preparação para os testes foram impedidos pelas barreiras de segurança da Urna Eletrônica.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.



TE PÚBLICO DE SEGURANÇA
DO SISTEMA ELETRÔNICO
DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Nada a declarar.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR:

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO — TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Individual – ROOT KIT JE-CONNECT

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	João Felipe Souza	08/03/2016 e 09/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	08/03/2016	Hora de início:	16:45	Hora de término:	11:39 do dia 09/03/2016
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

DADOS DO TESTE

Título do teste:	ROOT KIT JE-CONNECT.	
Início do teste (data/hora):	08/03/2016	16:45
Término do teste (data/hora):	09/03/2016	11:39
Critério de parada:	Alteração do voto.	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

Apresentou relaxamento no plano de teste ao solicitar o PIN do sistema JE-Connect.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TE PÚBLICO DE SEGURANÇA
DO SISTEMA ELETRÔNICO
DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

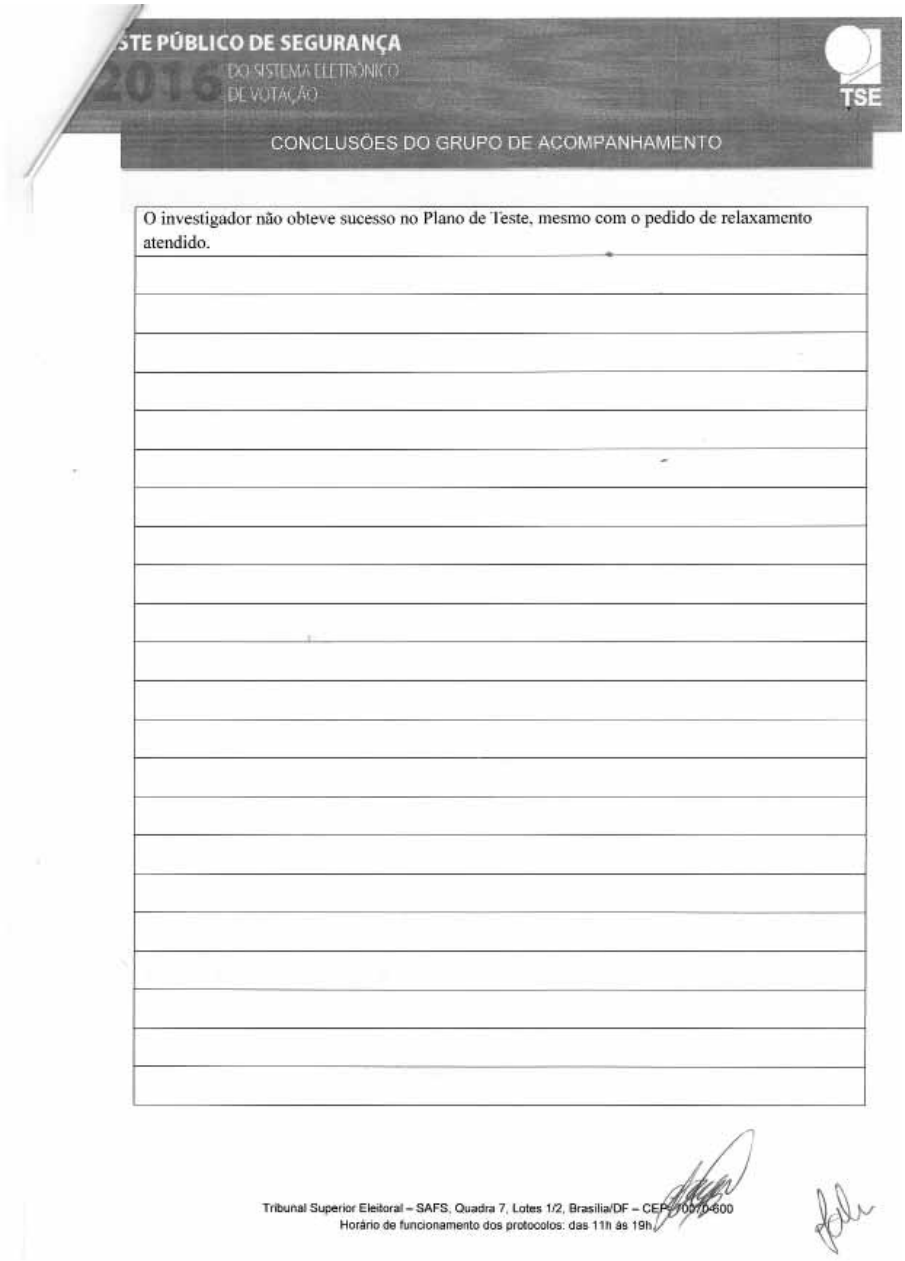
Etapa	Descrição	*Status*
1	Atacante obtém acesso ao pendrive do kit JE-Connect e ao pendrive da chave.	Executado.
2	Atacante utiliza o comando dd e realiza uma cópia dos dois pendrivers.	Executado.
3	Efetua-se a montagem da imagem do pendrive do kit JE-Connect.	Não foi a montagem do pendrive do JE-Connect.
4	Efetua-se a alteração da imagem do Linux, inserindo um rootkit com backdoor.	---
5	Inicializa-se o kit JE-Connect em uma máquina virtual.	---
6	Realiza-se o acesso remoto ao Kit JE-Connect, via código malicioso previamente inserido.	---
7	Obtém-se acesso à VPN de transmissão de dados.	---
8	Realiza-se teste de penetração no servidor RecArquivos e InfoArquivos.	---
9	Exploram-se vulnerabilidades (se encontradas) e alteram-se os votos.	---

STE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 08/03/2016>>
16:45	Investigador inicia o teste.
16:46	Analisa o JE-Connect no computador com UBUNTU.
16:55	Investigador faz cópia do JE-Connect usando o comando dd.
17:40	Encerra as atividades do dia.
---	<< É o que havia a ser relatado no acompanhamento do dia 08/03/2016 >>
---	<< Relato de acompanhamento de fatos relevantes do dia 09/03/2016 >>
09:30	Início dos testes do dia.
09:31	O investigador analisa o Kit JE-Connect conectado no computador com sistema operacional UBUNTU.
09:45	Inicia a cópia das informações do pendrive com o comando dd com sucesso para ao computador.
10:19	Análise das informações copiadas com o comando "hexdump -C".
10:41	Faz a cópia do Kit JE-Connect para dois pendrivers novos.
11:05	Cópia realizada com sucesso.
11:09	Boot pelo pendrive copiado em uma máquina teste, porém sem sucesso.
11:30	Boot do Kit JE-Connect com PIN fornecido pelo TSE.
11:39	Sem êxito, o investigador encerra os testes.
---	<< É o que havia a ser relatado no acompanhamento do dia 09/03/2016 >>

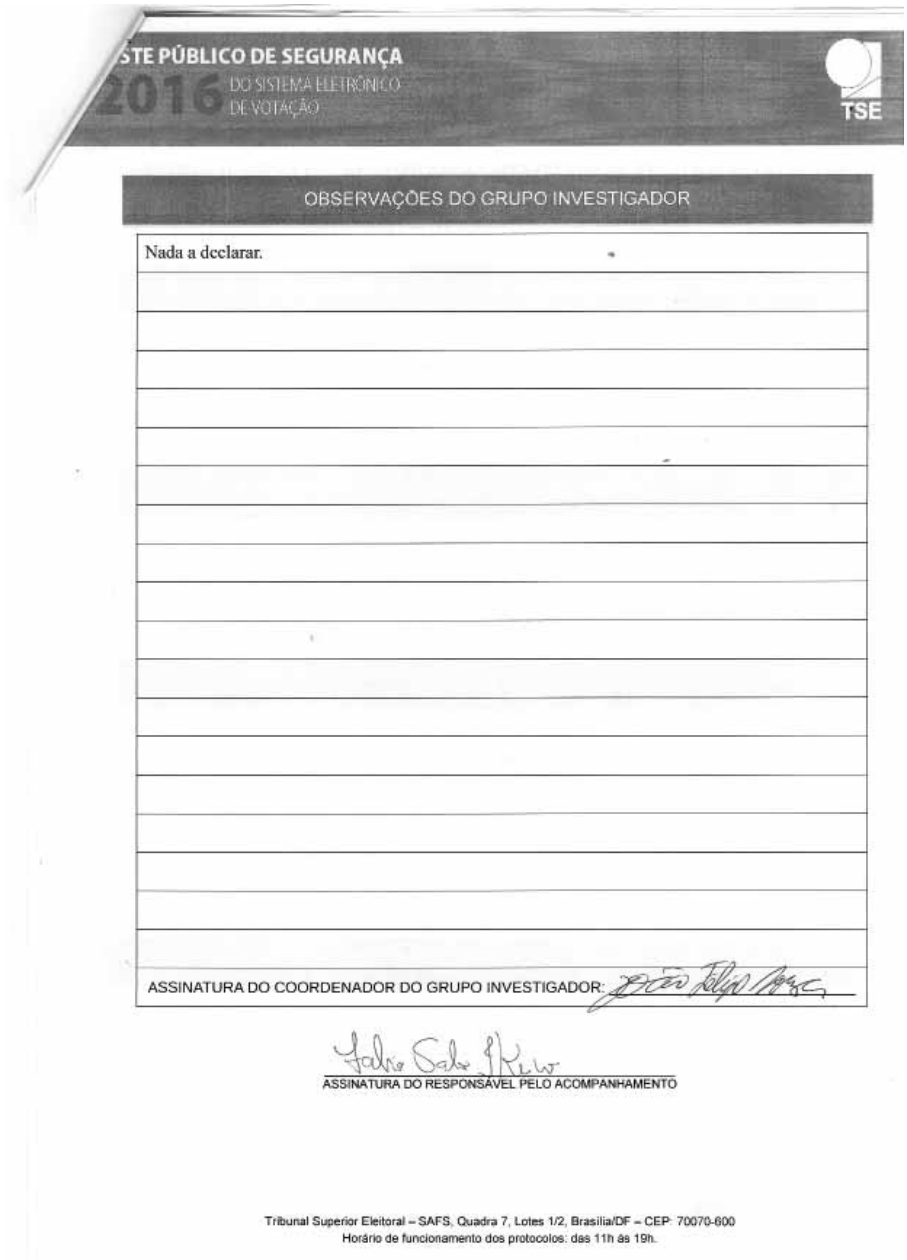


STE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

O investigador não obteve sucesso no Plano de Teste, mesmo com o pedido de relaxamento atendido.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h



STE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Nada a declarar.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR:

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

TESTE PÚBLICO DE SEGURANÇA
DO SISTEMA ELETRÔNICO DE VOTAÇÃO
2016
TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Individual – Reflash de Urna

DADOS DO GRUPO DE INVESTIGADORES

	Nome	Freq.
Investigador coordenador:	João Felipe Souza	10/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	10/03/2016	Hora de início:	14:05	Hora de término:	16:00
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

DADOS DO TESTE

Título do teste:	Reflash de Urna	
Início do teste (data/hora):	10/03/2016	14:05
Término do teste (data/hora):	09/03/2016	16:00
Critério de parada:		

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

1 - Lacre da Urna Eletrônica;
2 - Conivência dos mesários;
3 - Conivência dos fiscais.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

ESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	*Status*
	Preparação para as variações 01 e 02.	
1	Atacante obtém acesso ao flash dc carga e a memória de resultados da urna, antes das eleições.	Executado
2	Atacante realiza cópia da flash de carga e da memória de resultadós para uma imagem no computador através de cópia bloco a bloco (dd).	Executado
3	Depois da carga da urna, o atacante obtém acesso a urna para clonagem da flash interna e da flash de votação, bem como da memória de resultados.	Executado
	Variação 01	
4	Procede-se normalmente as eleições.	Executado
5	Ao término das eleições, atacante obtém cópia do livro com os eleitores presentes.	Executado
6	Realiza-se novo procedimento de carga da mesma urna eletrônica utilizando-se as memórias clonadas no passo 3.	Executado
7	Realiza-se procedimento simulado de votação com a urna eletrônica, desta vez, direcionando-se os votos.	Executado
8	Procede-se ao envio dos dados normalmente utilizando a MR gerada na eleição simulada.	Executado
9	Fim do teste.	Executado
	Variação 02	
4	No dia das eleições a urna oficial é levada para um local reservado com a finalidade de se realizar uma eleição simulada na urna oficial.	Executado
5	É levada para a eleição oficial uma urna qualquer, carregada com a memória gerada no passo 2 ou 3.	Executado
6	Equipe de apoio do atacante fornece em tempo real o título de eleitor dos votantes.	Executado
7	Atacante realiza votação simulada paralela e direcionada utilizando os números de títulos recebidos da equipe de apoio.	Executado
8	Ao término das eleições, o atacante substitui a mídia de resultados da urna qualquer utilizada na eleição real pela mídia da urna verdadeira que contém o resultado da eleição simulada. O mesmo ocorre com os boletins de urna impressos.	Executado

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

ESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 10/03/2016 >>
14:05	Investigador inicia o teste.
14:06	Investigador gera Mídia de Carga, Mídia de Votação e Mídia de Resultados no Gedai - UE
14:12	Investigador clona a Mídia de Carga, Mídia de Votação e Mídia de Resultados compilados com o comando dd.
14:15	Faz-se a carga de votação na Urna Eletrônica
14:23	Foi gerado o resumo de correspondência 084.936
14:25	O investigador tem acesso a Flash Interna e faz clone no computador com o comando dd.
14:29	Coloca a Flash Interna novamente na Urna Eletrônica.
14:30	Liga a Urna Eletrônica.
14:40	Com Flash de Carga e Mídia de Resultado, o investigador insere-as na Urna Eletrônica falsa. Resumo de correspondência da Urna Eletrônica falsa 160.079. Esta Urna Eletrônica será usada como Urna Eletrônica oficial.
14:42	A Urna Eletrônica falsa é carregada com Flash de votação clonada.
15:04	Início da eleição com eleitores reais votando na Urna Eletrônica clonada. Após cada voto do eleitor, o mesário repassa ao atacante o título do eleitor do votante. O atacante de posse dessa informação realiza o voto na Urna Eletrônica oficial.
15:08	Foram realizados mais 4 votos neste cenário.
15:20	A eleição é finalizada e gerados os BUs das duas Urnas Eletrônicas, oficial e clonada.
15:30	Para a transmissão dos resultados o atacante substitui a BU oficial pela fraudada (clonada).
15:30	Fim do teste V2.
15:40	Início do teste V1.
15:41	É realizado o reflash na Urna Eletrônica que já foi finalizada uma eleição utilizando as imagens clonadas no teste anterior.

ESTE PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

15:55	Realiza-se a eleição simulada com 5 votos.
16:00	Finaliza a eleição, o BU é impresso com o mesmo número de correspondência da eleição real.
---	<< É o que havia a ser relatado >>

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

Os testes foram bem sucedidos. Conclui-se que em um cenário real o teste implicaria em quebra de procedimentos, além de corrupção das pessoas envolvidas no processo eleitoral e ainda ter acesso a Urna Eletrônica.

OBSERVAÇÕES DO GRUPO INVESTIGADOR

O ataque pode ser prevenido adicionando-se um lacre a Flash Interna.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR:

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

TESTE PÚBLICO DE SEGURANÇA 2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

FORMULÁRIO DE ACOMPANHAMENTO DOS TESTES PÚBLICOS

Individual – Sequenciado de Votos

DADOS DO GRUPO DE INVESTIGADORES

Nome		Freq.
Investigador coordenador:	João Felipe Souza	10/03/2016

INFORMAÇÕES DO ACOMPANHAMENTO

Data:	10/03/2016	Hora de início:	17:30	Hora de término:	18:40
Resp. Acomp.:	Fabio Sato Ikuno			Rubrica:	

DADOS DO TESTE

Título do teste:	Sequenciador de votos.	
Início do teste (data/hora):	10/03/2016	17:30
Término do teste (data/hora):	10/03/2016	18:40
Critério de parada:	Quando conseguir quebrar o sigilo do voto do eleitor.	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

1 - Lacre da Urna Eletrônica;
2 - Conivência dos mesários;
3 - Conivência dos fiscais.

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

PÚBLICO DE SEGURANÇA
2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO
TSE

ETAPAS PROPOSTAS PARA O TESTE

Etapa	Descrição	Status
1	Atacante consegue acesso físico a urna depois de alguns votos registrados	Executado
2	Atacante retira flash de votação e flash interna da urna eletrônica.	Executado
3	Atacante copia os arquivos de registro digital do voto e de comparecimento utilizando um computador e um adaptador de flash card compatível com a memória da urna.	Executado
4	Atacante insere os cartões de memória de volta na urna.	Executado
5	Atacante espera o próximo voto.	Executado
6	Atacante retira novamente as memórias de votação.	Executado
7	Atacante copia os arquivos de registro digital do voto e de comparecimento.	Executado
8	Atacante aguarda o encerramento das eleições.	Executado
9	Utilizando as memórias geradas no passo 3, o atacante restaura o estado de memória da votação da urna ao instante do passo 2.	Executado
10	Atacante encerra a votação na urna e obtém o Resultado 1.	Executado
11	Utilizando as memórias geradas no passo 7, o atacante restaura o estado de memória da votação da urna ao instante do passo 6.	Executado
12	Atacante encerra a votação na urna e obtém o Resultado 2.	Executado
13	Atacante compara Resultado 1 com o Resultado 2 e identifica o voto do eleitor.	Executado

ACOMPANHAMENTO DOS FATOS

Hora	Fato
---	<< Relato de acompanhamento de fatos relevantes do dia 10/03/2016 >>
17:30	Início do teste.
17:31	Gerado Flash de Carga, Flash de Votação e Mídia de Resultado.
17:33	É dada carga na Urna Eletrônica.
17:35	Início da eleição.
17:45	São realizados dois votos válidos.
17:45	A Urna Eletrônica é desligada.
17:47	O investigador abre a Urna Eletrônica e retira a Flash Interna e as Mídias Externas.
17:48	Investigador faz dd dc todas as Mídias retiradas da Urna Eletrônica.
18:10	Retorna as Mídias à Urna Eletrônica.
18:11	Inicia-se novamente a votação (exige o código de reinício)
18:15	É realizado um voto.
18:16	É finalizada a votação com 3 votos. É impresso a BU.
18:18	O investigador grava as imagens geradas no tempo 17:48 com o comando dd nas flashes
18:20	O investigador abre a Urna Eletrônica e substitui as mídias originais pelas gravadas
18:22	A Urna Eletrônica é ligada
18:28	Após a Urna Eletrônica ser ligada, o investigador finaliza a votação com 2 votos. É impresso a BU
18:31	De posse das duas BUs, é possível saber qual foi o último voto. Para que o voto seja mapeado, é necessário verificar o último eleitor que votou.
	Com êxito, o investigador encerra os testes.
---	<< É o que havia a ser relatado >>

2016 DO SISTEMA ELETRÔNICO DE VOTAÇÃO

TSE

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO

Dado os relaxamentos solicitados pelo investigador, o teste obteve sucesso.
Conclui-se que em um cenário real o teste implicaria em quebra de procedimentos, além de corrupção das pessoas envolvidas no processo eleitoral e ainda ter acesso a Urna Eletrônica.
O investigador não incluiu no Plano de Teste no item 2.7, como ele mapearia a ordem que o eleitor votou.

OBSERVAÇÕES DO GRUPO INVESTIGADOR

Pode ser aprimorada a segurança da urna eletrônica por meio da adição de um lacre na Flash Interna. A violação deste lacre indica que a Urna Eletrônica foi aberta.

ASSINATURA DO COORDENADOR DO GRUPO INVESTIGADOR:

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Tribunal Superior Eleitoral – SAFS, Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600
Horário de funcionamento dos protocolos: das 11h às 19h.

Anexo G – Relatório da Comissão Avaliadora

Relatório da Comissão Avaliadora do Teste Público de Segurança 2016

1 Introdução

A Comissão Avaliadora designada pela Resolução TSE nº 23.444, de 30 de abril de 2015, possui as atribuições de validar a metodologia e os critérios de julgamento definidos para o Teste de Segurança.

O propósito deste relatório é apresentar os resultados dos testes dos investigadores e grupos de investigadores.

2 Metodologia

Foram disponibilizados componentes de *software* para a realização do teste cujas versões podem ser encontradas a seguir:

- JEConnect: 14.50
- Transportador: 16.2.4-TPS2016
- RecArquivos: 16.1.2-TPS2016
- InfoArquivos: 16.1.6-TPS2016
- GEDAI-UE versão 3.15.0.0 - Araticum e UENUX versão 5.12.0.0 – Araticum
- GEDAI-UE versão 3.16.1.0 - Mangueira 2 e UENUX versão 5.13.0.0 – Mangueira

Os critérios de análise para avaliação dos testes foram:

- Pontos de intervenção: elementos do processo eleitoral atacados
- Impacto: quais propriedades de segurança violadas
- Extensão: granularidade, extensão geográfica (ex. urna, seção, etc)
- Contexto: procedimentos, atores, circunstâncias do processo eleitoral

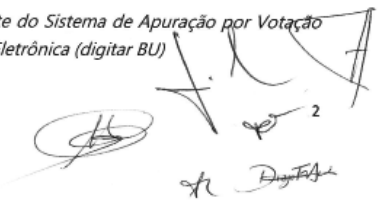
3 Planos de Teste

Os planos de teste apresentados em consequência ao edital dos Testes Públicos de Segurança do Sistema Eletrônico de Votação, pelos 4 grupos e 1 investigador individual totalizaram 11 propostas.

a. Planos de Teste não Realizados e não Avaliados
   i. Segue abaixo a relação dos indeferidos pela Comissão Reguladora por estarem em desacordo com o escopo definido para a investigação:
      1. Grupo 2: *Análise da segurança do armazenamento de arquivos e valores na memória da urna e nas mídias removíveis,*
      2. Grupo 2: *Análise de práticas de programação relacionadas ao uso de primitivas criptográficas e outros aspectos de segurança do código-fonte*
      3. Investigador Individual Marcelo Muzili: *Invasão no transporte dos dados no sistema de votação*

b. Planos de Teste Realizados e não Avaliados
   i. Os planos de teste executados, mas que não apresentaram contribuição relevante para o processo de aprimoramento do Sistema Eletrônico de Votação não foram avaliados por esta comissão.
      1. Grupo 2: *Ataque ao sigilo do voto*
      2. Grupo 4: *Tentativa de fraude na destinação dos votos na urna através de controle dos dispositivos de teclado e impressora*
      3. Investigador Individual João Felipe Souza: *Registrador do teclado, Destruidor de votos e Root Kit JE Connect*

c. Planos de Teste Realizados e Avaliados
   i. Os planos de teste executados, e que apresentaram contribuição relevante para o processo de aprimoramento do Sistema Eletrônico de Votação foram avaliados por esta comissão.
      1. Grupo 1: *Teste do Sistema de Apuração por Votação Totalmente Eletrônica (digitar BU)*



2. Grupo 5: *Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual*
3. Investigador Individual João Felipe Souza: *Reflash de urna*

4 Avaliação dos Planos de Teste Realizados e Avaliados

4.1 Grupo 1

1. Pontos de intervenção: elementos atacados

- Boletim de Urna (BU)

2. Impacto

- alteração do resultado de votação

3. Extensão

O ataque, como idealizado, afetaria o resultado de votação de uma seção eleitoral.

4. Análise contextual

Visualizam-se dois cenários para aplicabilidade do ataque proposto:

a) Atacante externo (não submetido a instruções da Justiça Eleitoral): o atacante gera um novo Boletim de Urna impresso, com votação falsa, mas com código verificador verdadeiro, e o encaminha para inserção no Sistema de Apuração (SA). Para isso, o atacante deve provocar situação de contingência, com eliminação da mídia de resultado, BU verdadeiro e/ou urna.

b) Atacante interno (submetido a instruções da Justiça Eleitoral): o atacante insere votação falsa com código verificador

verdadeiro no Sistema de Apuração (SA). Para isso, o atacante deve provocar situação de contingência, com eliminação da mídia de resultado, BU verdadeiro e/ou urna.

Pré-requisitos para o sucesso do ataque:

1) Conhecimento sobre como é calculado o código verificador
2) Acesso a um BU legítimo
3) Acesso a uma urna em modo SA
4) Interceptação e eliminação do BU verdadeiro e mídia de resultado

4.2 Grupo 5

1. Pontos de intervenção: elementos atacados

- saída de áudio
- terminal do mesário

2. Impacto

- quebra de sigilo de voto com áudio habilitado

3. Extensão

A quebra de sigilo, nesta proposta, poderá ocorrer em duas hipóteses:

a) Voto a voto, em qualquer urna, mediante habilitação de áudio pelo terminal do mesário;

b) Todos os votos de uma seção PNE.

4. Análise contextual

Visualizam-se três cenários para aplicabilidade do ataque proposto:

a) Quebra de sigilo de voto pelo próprio eleitor: o eleitor afirma ser PNE, conecta um transmissor na saída de áudio, o mesário o habilita como PNE, o voto é capturado pelo receptor;

b) Quebra de sigilo de voto pelo mesário: o mesário conecta um transmissor na saída de áudio, habilita o áudio para eleitores de interesse, o áudio é captado pelo receptor;

c) Quebra de sigilo de voto de todos os votos da seção especial para PNE: alguém conecta um transmissor na saída de áudio. Como há prévia habilitação do áudio, todos os votos são capturados pelo receptor.

Pré-requisitos para o sucesso do ataque:

a) Acesso à saída de áudio da urna
b) A saída de áudio deve ser habilitada

4.3 Investigador Individual João Felipe Souza

1. Pontos de intervenção: elementos atacados

- memória flash interna e mídias externas

2. Impacto

- quebra de sigilo do último voto computado antes da retirada de memória flash

3. Extensão

A quebra de sigilo, nesta proposta, poderá ocorrer sempre que houver a interrupção da votação e troca da memória flash.

4. Análise contextual

Visualiza-se um cenário para aplicabilidade do ataque proposto:

a) O atacante deve interromper a votação, desligar a urna, abri-la, retirar as memórias flash, fazer cópia. Após, deve reiniciar a votação com o código de reinício, computar o último voto e encerrar a votação. Em seguida, deve restaurar as memórias flash para o estado anterior e encerrar novamente. O último voto pode ser deduzido pela comparação dos dois BU.

Pré-requisitos para o sucesso do ataque:

1) Acesso físico irrestrito à urna
2) Violação do lacre

5 Recomendações

1) Implantar Processo Seguro Certificado de Desenvolvimento de Software

2) Revisão da abrangência e necessidade do termo de confidencialidade

3) A lacração dos sistemas deve ocorrer antes da inspeção dos códigos-fonte, que antecede a apresentação do plano de teste

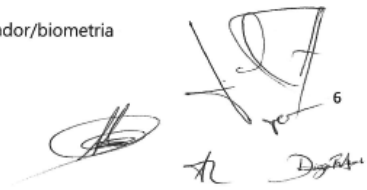
4) Permitir quaisquer membros das equipes admitidas para realizar plano de teste a elaboração de novos planos de testes adequados ao ambiente já disponibilizado pelo TSE

5) Realização de divulgação diária parcial dos testes já concluídos

6) Maior participação da Comissão Avaliadora durante a concepção, planejamento e execução do TPS

7) Criação de Comissão Mista Permanente, composta por componentes das quatro comissões do TPS 2016

8) TPS abranger o sistema totalizador/biometria



9) Eliminar restrição etária para participação no TPS

10) Instituir fórum técnico sobre o processo eleitoral, com colaboração direta da Comissão Mista Permanente

Brasília-DF, 11 de março de 2016.

Ana Lúcia Andrade de Aguiar
TSE

Jamil Salem Barbar
Comunidade Acadêmica (UFU)

Mamede Lima-Marques
Comunidade Acadêmica (UnB)

Diego de Freitas Aranha
SBC

Thiago de Sá Cavalcanti
Perito Criminal Federal

Antônio de Souza Dantas
Congresso Nacional

Osvaldo Catsumi Imamura
CTA

Lúcio Ivar do Sul
CONFEA

7

Esta obra foi composta na fonte Myriad Pro, corpo 10
e entrelinhas de 12 pontos, em papel AP 75g/m^2 (miolo)
e papel Cartão Supremo 250g/m^2 (capa).