



RELAÇÃO DOS PLANOS DE TESTE APROVADO APÓS RECURSO

Em atendimento ao Marco 10, mencionado no art. 21 do edito do Teste Público de Segurança 2017, torna-se publica a relação dos planos de teste aprovados após recurso.

Os investigadores e(ou) grupo de investigadores com inscrição aprovada devem atentar-se aos prazos e fases constantes do calendário do eventos, bem como observar art. 31 o edital, que lista os materiais e equipamentos disponibilizados pelo Tribunal Superior Eleitoral. Qualquer item necessário à execução dos testes e não contemplado pelo aludido dispositivo deverá ser provido pelo próprio participante.



I1 Cassio Goldschmidt			
Planos de Teste			
ID	Título	Resumo	Resultado
I1.1	Revisão de código e teste dinâmico de Geração das mídias para a preparação da urna eletrônica (GEDAI-UE)	Encontrar erros no GEDAI-UE que resultem em injeção de código ou afetem a disponibilidade, integridade ou confidencialidade.	APROVADO

I10 Jose Carlos Gama Quirino			
Planos de Teste			
ID	Título	Resumo	Resultado
I10.1	Ataque aos sistemas dos Hardwares e Softwares da urna eletrônica.	Contribuição da sociedade na identificação de possíveis vulnerabilidades e falhas realizadas, violação da integridade ou do anonimato dos votos e as soluções de aperfeiçoamento ao sistema. Tendo como objetivo burlar códigos de verificações impressos no boletim da urna e a quebra do sigilo do voto baseado em gravação de áudio para deficientes visuais.	APROVADO

I13 Marcelo dos Anjos			
Planos de Teste			
ID	Título	Resumo	Resultado
I13.1	Teste Invasão Hardware / Software parte 1 HARDWARE	Alteração do sistema de Segurança por Hardware da Urna.	APROVADO
I13.2	Teste Invasão Hardware / Software parte 2 SOFTWARE	Alteração de dados no sistema de envio transportador, com invasão do ambiente seguro linux, proporcionado pelo JE connect.	APROVADO

I15 Rodrigo Cardoso Silva			
Planos de Teste			
ID	Título	Resumo	Resultado
I15.1	Programa Transportador de Arquivos - "Teste Doodle"	Simulação do envio de um número de MRs mediante um microcomputador do cartório eleitoral para um servidor receptor (data centers) do TRE e\ou TSE (o servidor ainda não está claro) para verificar e descobrir a URL para, assim, afetar o ambiente de transmissão.	APROVADO COM RESSALVA Em atendimento ao art. 2º, § 2º, inciso VII e ao art. 31, inciso V do edital do TPS 2017, devem ser suprimidas do plano de teste ações que visem a ataques do tipo negação de serviço ou que necessitem de acesso à Internet.
I15.2	UENUX e softwares básicos "Metamorfose (Kafka)"	Tentar explorar as vulnerabilidades da versão do Kernel utilizado na UE2015 e suas respectivas bibliotecas e drivers, com a possibilidade da utilização de um programa, pois mesmo para qualquer aplicação existente e que esteja segura, ela ainda depende do OS.	APROVADO

G1 Diego de Freitas Aranha			
Componentes			
Caio Lúders de Araujo Paulo Matias Pedro Yóssis Silva Barbosa Thiago Nunes Coelho Cardoso			
Planos de Teste			
ID	Título	Resumo	Resultado
G1.1	Captura de chaves criptográficas do Flash de Carga	O teste proposto objetiva recuperar as chaves criptográficas do Flash de Carga para permitir acesso a informações críticas armazenadas na partição cifrada do cartão.	APROVADO
G1.2	Execução remota de código na plataforma web (RecArquivos e InfoArquivos)	O teste proposto tem como objetivo a execução de código arbitrário nas plataformas web de recebimento de arquivos e de informações de totalização.	APROVADO
G1.3	Tentativa de violação do sigilo do voto	O teste proposto objetiva verificar se eleições distintas produzem arquivos com Registro Digital do Voto (RDV) com ordens de permutação dos votos também distintas e também determinar a qualidade do gerador de números aleatórios utilizado no sistema.	APROVADO
G1.4	Inserção de dispositivo USB malicioso	O teste proposto objetiva avaliar qual acesso um dispositivo USB malicioso inserido na urna poderia obter a subsistemas de software básico ou de hardware.	APROVADO



G3	Luis Antonio Brasil Kowada		
Componentes			
Gabriel Cardoso de Carvalho Ramon Rocha Rezende Victor Faria de Souza			
Planos de Teste			
ID	Título	Resumo	Resultado
G3.1	Análise do uso dos procedimentos criptográficos	Este teste visa avaliar se os procedimentos e gerenciamento de chaves garantem a confidencialidade e autenticação.	APROVADO

G4 Ivo de Carvalho Peixinho

Componentes

Fabio Caus Sicoli
Paulo Cesar Hermann Wanner

Nota: por decisão da comissão reguladora do TPS e em atendimento à solicitação do Sr. Ivo de Carvalho Peixinho, as inscrições individuais deste e dos componentes citados acima foram agrupadas e convertidas em inscrição em grupo.

Planos de Teste

ID	Título	Resumo	Resultado
G4.1	Extração de chave privada do Sistema Operacional da Urna Eletrônica	<ul style="list-style-type: none">1- Gerar um cartão compactflash a partir do GEDAI-UE2- Alterar o master boot record (MBR) para permitir o carregamento do bootloader3- Abrir o cartão em uma ferramenta disassembler4- Alterar as checagens de integridade saltando (JMP) para o código seguinte5- Corrigir eventuais drivers do kernel para permitir a inicialização em um PC comum6- Alterar o init para inicializar um shell ao invés do GAP7- Inicializar o sistema operacional da urna eletrônica em um computador desktop8- Resgatar a chave privada no sistema de arquivos criptografado	APROVADO