Relatório da Comissão Avaliadora sobre Confirmação das Correções

1. Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 601 de 7 de agosto de 2019, tem como atribuição validar a metodologia e os critérios de julgamento definidos no Edital do TPS e avaliar e homologar os resultados obtidos durante o teste. Cabe a ela, ao final, produzir relatório conclusivo contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes porventura identificadas. A Comissão também avalia as atividades do evento de confirmação, por parte dos investigadores, das correções efetuadas pelo TSE

A Comissão é composta de 10 membros, representantes dos seguintes órgãos:

1. TSE – SANDRO VIEIRA
2. MPF – LUIS OTÁVIO DE COLLA FURQUIM
3. Congresso Nacional – FREDERICO QUADROS D´ALMEIDA
4. OAB – JOSÉ RORILSON VIEIRA ARAÚJO
5. PF – PCF MARCELO ANTONIO DA SILVA
6. CONFEA – RODRIGO DE SOUZA BORGES
7. SBC – PAULO LÍCIO DE GEUS
8. Comunidade Acadêmica – MAMEDE LIMA MARQUES
9. Comunidade Acadêmica – OSVALDO CATSUMI IMAMURA
10. Comunidade Acadêmica – JAMIL SALEM BARBAR

O propósito deste relatório sucinto é comentar sobre as atividades do evento de confirmação das correções.

2. Avaliação das correções implementadas pelo TSE e confirmação pelos investigadores

2.1) Grupo Paulo César Herrmann Wanner

Quebra da criptografia de proteção do sistema gerador de mídia das urnas eletrônicas.

1. Contexto:

   A quebra da cifragem do armazenamento da máquina que roda o SIS havia sido facilitada no TPS2019 pela presença de parte da chave digital disposta no código fonte. A partir disso, a localização de tal parte dessa chave dentro do armazenamento e consequente referências a tal conteúdo, permitiu levantar os demais trechos de código responsáveis por coletar as parcelas restantes da chave espalhada e assim decifrar a imagem do armazenamento do SIS. Assim, as modificações laterais ao GEDAI permitiram alterar algumas informações não críticas do BU (Boletim de Urna) impresso,

sem contudo ser possível alterar as mesmas informações no arquivo do BU, o qual é criptografado por outro mecanismo para ser transportado para totalização .

2. Melhorias efetuadas pelo TSE:
    - Remoção dos fragmentos presentes no código fonte, tornando a busca dos fragmentos da chave bem mais difícil;
    - Detecção e bloqueio de execução em máquina virtual, via driver em espaço de kernel, a fim de dificultar os procedimentos de obtenção dos fragmentos de chave e demais informações relevantes para ataque à cifragem do armazenamento;
    - Bloqueio de *dumps* de hibernação e de *crash*, para dificultar por outros meios a obtenção dos dados já mencionados anteriormente;
    - Melhor validação do SIS pelas aplicações, para melhorar o controle de acesso.

3. Contribuição:

    De posse do conhecimento de funcionamento da urna, os investigadores conseguiram vencer as barreiras extras impostas e quebraram a cifragem do armazenamento; embora utilizando-se de recursos tecnológicos mais complexos.

    Apesar de não se conseguir neste teste de confirmação a eliminação da vulnerabilidade detectada pelos investigadores, percebe-se que, dentro das possibilidades tecnológicas, as modificações introduzidas cumpriram seu intento, exigindo mais recursos dos investigadores para obtenção do marco alcançado.
    Importante observar que o ambiente onde roda o SIS é externo à urna, que por sua vez cumpre o papel de reforçar a segurança da aplicação GEDAI. Assim, tal ambiente está sujeito às regras de funcionamento, permissionamento e usabilidade do sistema operacional Windows, forçando uma solução de compromisso entre segurança e usabilidade/logística de uso no SVE.

    Ressalte-se também a capacitação da equipe de investigadores, que conseguiu suplantar as novas barreiras apesar do exíguo tempo disponibilizado pelo evento de confirmação das correções introduzidas.

4. Impactos:

    A cifra da mídia de armazenamento foi comprometida, eliminando uma barreira que dificulta ataques contra o sistema de segurança SIS, fazendo com que haja acesso ao ambiente onde roda a aplicação GEDAI.

    Contudo, apesar de os investigadores terem em mãos o mesmo estado que os permitiu introduzir algumas adulterações na versão impressa do BU no TPS em 2019 (embora não na versão que é enviada ao sistema totalizador), modificações foram feitas pelo TSE no sentido de eliminar tais oportunidades, mesmo que não danosas ao processo de totalização. Os arquivos auxiliares que continham tais informações, para o BU impresso, foram eliminados e estas últimas agora obtidas da fonte original dentro do programa da urna, da mesma forma como é feita a geração do BU fornecido ao processo de totalização.

    Além do mais, todo o processo de geração e manipulação de chaves, interação com o TPM e o envolvimento do sistema operacional Windows foi refeito, padronizando os métodos de acesso e tornando o conjunto muito mais robusto, de acordo com as descrições das alterações fornecidas pela equipe do TSE.

2.2) Investigador Leonardo Cunha dos Santos (não presente ao evento de confirmação)

Falha do teclado, que provocava travamento da urna, e o uso indiscriminado, para procedimentos preparatórios e possíveis situações de falhas, do sinal sonoro popularmente reconhecido pelos usuários como voto inserido na urna.

1. Contexto:

   No TPS em 2019 um investigador descobriu que a desconexão do teclado da urna, seja por mau contato ou intencional, provocava travamento da urna. A equipe do TSE identificou que tal falha era identificada mas não processada apropriadamente, apesar da urna continuar operando internamente.

   Além disso, o investigador sugeriu que o sinal sonoro característico da urna era usado indistintamente para todas as situações na urna. Como a fase de início da votação pela mesa envolve várias confirmações de atividades preparatórias, eleitores enfileirados aguardando o início da votação, desconhecedores dos procedimentos iniciais, poderiam concluir que se estaria inserindo votos ilegítimos na urna previamente ao início da votação.

2. Melhorias efetuadas pelo TSE:

   O evento de desconexão do teclado agora é corretamente tratado como exceção e reportado. Desta forma, em face do evento, os mesários saberão porque a urna efetivamente ficou inoperante, acionando apropriadamente a reposição da mesma.

   Com relação ao sinal sonoro, foram introduzidos sinais diferenciados para os diferentes tipos de situação, de forma a preservar o som conhecido dos eleitores exclusivamente para a confirmação do voto.

3. Contribuição:

   Não houve participação efetiva do investigador neste evento de confirmação do TPS, porém reporta-se aqui o que foi feito a respeito.

3. Conclusão

Tendo em vista os resultados dos investigadores e as características intrínsecas do ambiente do SVE, esta comissão entende que as alterações realizadas pela equipe técnica do TSE atenderam plenamente a melhoria dos quesitos de vulnerabilidade de segurança apontados pelos investigadores, por ocasião do TPS em novembro de 2019.

Brasília/DF, 31 de agosto de 2020.

COMISSÃO AVALIADORA DO TESTE PÚBLICO DE SEGURANÇA 2019