Tribunal Superior Eleitoral

2019

Vulnerabilidades e sugestões de melhorias encontradas no Teste Público de Segurança 2019

RELATÓRIO TÉCNICO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Introdução

O Teste Público de Segurança - TPS, que este ano chegou à sua quinta edição, é um dos marcos do processo de desenvolvimento dos sistemas eleitorais e do hardware da urna eletrônica. Ao longo dos últimos anos, a cada edição do TPS foi possível aprimorar os sistemas eleitorais que seriam utilizados nas eleições subsequentes, que passaram a contar com hardware e software mais seguros e robustos.

A edição de 2019 do TPS contou com um grande número de pesquisadores e profissionais altamente qualificados. E mais uma vez, foram encontrados achados relevantes de segurança e usabilidade nos sistemas.

Este relatório tem por objetivo apresentar os planos de teste que foram executados pelos investigadores durante o evento, que ofereceram algum tipo de contribuição. É feita uma breve descrição dos trabalhos apresentados, dos resultados obtidos e das falhas que deram causa ao sucesso dos achados.

Sempre que possível, os achados são colocados no contexto real de exploração da vulnerabilidade apresentada. Este relatório não tem o objetivo de desqualificar ou minimizar o trabalho dos investigadores, mas sim dar aos achados a dimensão adequada e evitar que sejam feitas especulações indevidas sobre o potencial de um ataque. Todos os achados do TPS são importantes e precisam ser devidamente tratados, pois afetam algumas das barreiras de segurança do processo eleitoral, direta ou indiretamente.

A análise feita neste relatório está limitada ao conjunto de software do Ecossistema da Urna e ao Subsistema de Instalação e Segurança – SIS. Destaca-se que o conjunto de software do Ecossistema da Urna é composto por todo o software executado pela urna eletrônica, conhecido como Uenux (composto por *bootloader*, kernel do Linux, drivers, bibliotecas e aplicativos), e pelo software de geração de mídias para a urna (Gedai-UE). O SIS é um conjunto de aplicações e drivers para o sistema operacional Windows, responsáveis por criar uma infraestrutura de segurança e controle de acesso às aplicações da Justiça Eleitoral para a plataforma desktop.

Ao final do relatório são apresentadas as ações levantadas que visam à mitigação dos achados do TPS 2019.

O objetivo deste documento é apresentar a visão da equipe técnica do TSE, tanto dos trabalhos realizados durante o TPS, quanto daquilo que precisa ser feito para mitigação das vulnerabilidades. Este documento não se sobrepõe ao relatório da Comissão Avaliadora do TPS, tampouco aos registros realizados pela equipe de acompanhamento e pelos próprios investigadores.

Na verdade, espera-se justamente a conjunção das visões do TSE, da Comissão Avaliadora, dos investigadores e da comunidade técnico-científica para a construção de sistemas eleitorais cada vez mais seguros.

Análise dos planos de teste executados

A seguir é feita uma análise dos trabalhos realizados durante o TPS 2019, tendo como referência os planos de teste apresentados pelos investigadores durante a fase de inscrição[1].

Grupo G5

O grupo liderado por Paulo Cesar Hermann Wanner contava também com a participação de Ivo Peixinho e Galileu Batista de Souza, todos peritos da Polícia Federal. Eles apresentaram três planos de teste: **G5.1 – Extração de dados e configurações do Kit JE Connect**; **G5.2 – Extração do conteúdo do disco criptografado do SIS** e **G5.3 – Instalação e execução de código arbitrário em uma máquina do GEDAI para implante de dados falsos na Urna Eletrônica**.

Os investigadores procederam então com o emprego de técnicas de engenharia reversa para a obtenção da chave do disco criptografado do SIS, tendo controle sobre a instalação do Gedai-UE e, dessa forma, sendo bem-sucedidos ao final do TPS sobre os planos G5.2 e G5.3. Os investigadores não obtiveram êxito na execução do plano G5.1.

Pelo nível de acesso aos equipamentos atacados (computadores presentes dentro das instalações da Justiça Eleitoral) e o relaxamento de algumas barreiras de segurança (fornecimento da senha de configuração do BIOS e senhas de usuários locais), os ataques realizados pelo grupo podem ser classificados como de origem interna.

A. Extração do conteúdo do disco criptografado do SIS

O primeiro passo foi a inicialização com um LIVE CD para cópia do disco cifrado e dump do registry do Windows para mídia removível. A senha da BIOS foi fornecida aos investigadores. Após concessão pela equipe técnica, com a utilização de um LIVE CD com o sistema operacional Kali, foi realizada uma cópia de arquivos e registros da estação do SIS.

Em seguida, partiu-se para a montagem do disco cifrado usando as informações do registro do Windows e o programa Truecrypt. De posse dos arquivos extraídos anteriormente, foram realizadas tentativas de montagem do disco criptografado, utilizando informações retiradas do registro e da análise dos códigos fontes, mas sem sucesso.

O próximo passo foi realizar cópia do disco e inicialização em uma máquina virtual para realizar dump de memória. Utilizando o LIVE CD com o sistema operacional Kali, foi criada uma cópia do disco para ser utilizada em ambiente virtual. Nesse ambiente virtual foi realizado um despejo (dump) completo de memória. De posse desse arquivo de dump, foram realizadas diversas tentativas de localização das chaves, utilizando as ferramentas Volatility e Truecrypt, mas sem sucesso.

Em seguida, os investigadores utilizaram um editor hexadecimal para visualizar o arquivo de dump de memória. Passaram então a procurar por fragmentos das chaves, que por sua vez foram encontrados na consulta ao código-fonte do SIS. Dessa forma, foram capazes de recuperar a chave do disco criptografado do SIS.

Finalmente, partiram para a montagem do disco cifrado e cópia dos arquivos sensíveis. De posse do arquivo de imagem de disco e da chave, foi possível montar o disco criptografado fora do ambiente SIS, e por consequência, a captura dos arquivos do Gedai-UE.

[1] http://www.justicaeleitoral.jus.br/tps/arquivos/tps-planos-de-testes-aprovados.pdf

B. Instalação e execução de código arbitrário em uma máquina do GEDAI para implante de dados falsos na Urna Eletrônica

Uma vez tendo acesso aos arquivos da instalação do Gedai-UE, os investigadores investiram na tentativa de uso de chaves privadas usadas para assinatura de arquivos para a urna e outros arquivos sob guarda da aplicação.

Os investigadores localizaram o arquivo chaveiro.pri, que guarda de forma ofuscada a chave que protege as demais chaves utilizadas pelo Gedai-UE[2]. Analisando o código-fonte do Gedai-UE, os investigadores foram capazes de reverter a operação de XOR que ofuscava o chaveiro.pri e, com isso, foram capazes de decifrar a chave sevin_GEDAI.ber.pri. Essa chave é utilizada para assinar arquivos gerados pelo Gedai-UE para a urna.

A chave sevin_GEDAI.ber.pri não foi utilizada diretamente pelo grupo. Essa chave é utilizada pelo algoritmo de assinatura digital fornecido pelo Cepesc/Abin. Por se tratar de Algoritmo de Estado, o acesso a uma aplicação ou biblioteca que implemente essa assinatura é de caráter restrito[3]. Incapazes de usar a chave diretamente, os investigadores passaram a tentar manipular a instalação do Gedai-UE para que o software assinasse dados modificados para a urna.

As tentativas de execução do Gedai-UE fora de uma instalação Windows com SIS não foram bem-sucedidas. Por outro lado, uma instalação SIS legítima, mas com as proteções desativadas, permitiu a execução normal do Gedai-UE. Para avançar nessa linha, o grupo usou novamente o Kali para desativar os mecanismos de controle de acesso do SIS.

A primeira tentativa se deu sobre o banco de dados SQLite do Gedai-UE. Esse banco de dados não é assinado digitalmente. Os investigadores conseguiram alterar um registro do banco, mas como este não guarda dados que são carregados na urna, essa modificação não produziu qualquer efeito.

Em seguida, utilizando o debugger x64dbg, os investigadores foram capazes de entender o processo de geração de mídias de carga e, com isso, modificar um dos arquivos gerados pelo Gedai-UE para a urna. Os investigadores foram capazes de alterar o que seria gravado no arquivo *lo.dat. Esse arquivo agrupa dados relativos à unidade da federação (UF), município, zona e local de votação de uma determinada seção eleitoral. Os investigadores foram capazes de alterar a sigla da UF e o nome do município. O Gedai-UE assinou o arquivo modificado, que foi carregado com sucesso pelo software da urna. Os dados modificados foram apresentados em telas e relatórios da urna. Trata-se, portanto, de um ataque de descaracterização, facilmente identificável durante o processo de preparação da urna para a eleição, e que não modifica o comportamento do software.

Contrariando as expectativas dos investigadores, eles não foram capazes de alterar dados de eleitores e candidatos. Isso porque esses dados são assinados pelos sistemas responsáveis pelo cadastro de eleitores e registro de candidaturas, respectivamente. O Gedai-UE apenas repassa esses arquivos para urna, sem qualquer tipo de modificação. Todas as tentativas de manipulação de dados de eleitores ou candidatos foram prontamente identificadas pela urna.

Investigador I2

O investigador Leonardo Cunha dos Santos apresentou o plano **I2 – Teste de invasão utilizando análise instantânea de pulso elétrico**. Embora o investigador não tenha obtido sucesso em suas tentativas de identificação de padrões em circuitos elétricos da urna, sobretudo o teclado do terminal do eleitor, a sua análise levantou sugestões importantes.

[2] É utilizada criptografia AES CBC de 256 bits para a proteção das chaves.
[3] Os investigadores solicitaram a entrega de ferramenta de assinatura para uso da chave, mas o pedido foi negado pela Comissão Reguladora do TPS, por se tratar de Algoritmo de Estado. Por outro lado, o código-fonte da biblioteca do Cepesc/Abin estava amplamente disponível para verificação no ambiente de inspeção de código-fonte.

Uma das sugestões apresentadas foi que o software da urna sinalize para o operador que teclado do terminal do eleitor perdeu comunicação com a placa-mãe da urna. Outra sugestão foi utilizar o sinal sonoro de fim da votação exclusivamente para esse fim – o investigador observou que o mesmo sinal sonoro é utilizado quando a urna é desligada na chave.

Respostas aos achados do TPS

A edição de 2019 do TPS mais uma vez trouxe um número significativo de contribuições para o aperfeiçoamento do conjunto de software do Ecossistema da Urna, sobretudo para a plataforma desktop. Todos os achados descritos anteriormente serão tratados até a conclusão do desenvolvimento do software que será utilizado nas Eleições 2020.

As respostas receberam a seguinte classificação:

- **Curto prazo (C)**: conclusão até a primeira quinzena de janeiro.
- **Médio prazo (M)**: conclusão até o Teste de Confirmação (final de abril).
- **Longo prazo (L)**: conclusão até a lacração das Eleições 2020.
- **Pós 2020 (P)**: conclusão após a lacração das Eleições 2020 (tratam-se de evoluções mais robustas sobre as ações anteriores).

Todas as ações dizem respeito ao software baseado naquele que foi apresentado no TPS 2019, cuja evolução resultará no software a ser utilizado nas Eleições 2020. Segue a lista de achados do TPS seguida das respectivas ações.

A. Chaves do disco criptografado do SIS disponível no ambiente de inspeção de código:
1. Segregação das chaves contidas no código-fonte em headers separados (C).
2. Retirada das chaves contidas no código-fonte (M).

B. Execução do SIS em máquina virtual:
1. Detecção e bloqueio via driver em espaço de kernel (M).

C. Criação de dumps de memória:
1. Impedir dumps de hibernação (M).
2. Impedir dumps de crash (M).
3. Analisar paginação de memória (L).

D. Superação dos controles de acesso do SIS:
1. Montagem da unidade criptografada sob demanda (M).
2. Autenticação entre SIS e Gedai-UE (M).

E. Modificação de dados no Gedai-UE para a urna:
1. Redução do conjunto de dados gravados em arquivos pelo Gedai-UE – uso de dados previamente assinados sempre que possível (M).
2. Assinatura do banco de dados SQLite do Gedai-UE (C).

F. Execução do Gedai-UE em máquina virtual:
1. Detecção e bloqueio de execução na aplicação (M).

G. Execução do Gedai-UE sob debugger:
1. Detecção e bloqueio de execução na aplicação (M).

H. Acesso a chaves do Gedai-UE:
1. Mecanismo de proteção por software (M).
2. Mecanismo de proteção por hardware (P).

I. Perda de comunicação com o teclado do terminal do eleitor:
1. Detecção e alerta ao operador (M).

J. Sinal sonoro do fim de votação usado para outros fins:
1. Substituição dos sinais sonoros coincidentes com o fim de votação (C).

A lista de ações apresentada não é definitiva e poderá sofrer alterações ao longo do processo de desenvolvimento. De qualquer forma, a sua implantação poderá ser auditada pelos mecanismos previstos na

resolução de fiscalização das eleições, em especial durante os seis meses que antecedem a Cerimônia de Lacração e Assinatura Digital dos Sistemas Eleitorais e durante a cerimônia em si.

Os investigadores também serão convocados oportunamente para verificar as correções implementadas e executar novamente os seus planos de teste, com vistas a comprovar que as falhas foram tratadas.

Conclusão

A edição do TPS de 2019 contou com a presença de pesquisadores e profissionais altamente qualificados em técnicas de criptografia, desenvolvimento de software seguro, microeletrônica e engenharia reversa. Os achados dos investigadores provocarão correções e melhorias fundamentais para que o SIS e o conjunto de software do Ecossistema da Urna estejam num patamar ainda mais elevado de segurança e robustez para as Eleições 2020.

As ações apresentadas aqui para a mitigação das falhas encontradas serão implementadas a tempo das Eleições 2020, incluindo até uma trilha de evolução após as próximas eleições. A equipe técnica da Secretaria de Tecnologia da Informação entende, contudo, que as ações listadas neste documento podem não ser definitivas e está aberta a sugestões dos próprios investigadores e da comunidade técnico-científica em geral.