TESTE PÚBLICO DE SEGURANÇA 2021

6ª EDIÇÃO • 22 a 26 DE NOVEMBRO DE 2021 •

TSE

Relatório Técnico de Avaliação Geral do TPS

Tribunal Superior Eleitoral
22 a 26 de novembro de 2021

CONTEÚDO

LISTA DE ACRÔNIMOS

ADH	Ajuste de Data e Hora
ATUE	Aplicativo de Teste da Urna Eletrônica
BU	Boletim de Urna
GAP	Gerenciador de Aplicativos
GEDAI-UE	Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica
JE	Justiça Eleitoral
LARC	Laboratório de Arquitetura e Redes de Computadores
MC	Mídia de Carga
ME	Mídia Externa
MI	Mídia Interna
MR	Mídia de Resultados
MV	Mídia de Votação
PCS	Departamento de Engenharia de Computação e Sistemas Digitais
RDV	Registro Digital do Voto
RED	Sistema de Recuperação de Dados
ROM	*Read-Only Memory*
SEINT	Seção de Integração de Sistemas Eleitorais
SETOT	Seção de Totalização e Divulgação de Resultados
SEVIN	Seção de Voto Informatizado
STE	Sistema de Teste Exaustivo
TE	Terminal do Eleitor
TM	Terminal do Mesário
TPS	Teste Público de Segurança
TRE	Tribunal Regional Eleitoral
TSE	Tribunal Superior Eleitoral
UE	Urna Eletrônica
USP	Universidade de São Paulo
VPP	Verificação Pré/Pós-Eleição

INTRODUÇÃO

A 6ª edição do Teste Público de Segurança – TPS aconteceu no período de 22 a 27 de novembro de 2021 no Tribunal Superior Eleitoral.

O TPS deste ano trouxe as seguintes inovações:

- Ampliação do escopo dos sistemas a serem avaliados, com a inclusão dos os sistemas de apoio à auditoria de funcionamento das urnas no dia da votação (Módulo Sorteio); os sistemas de apoio à auditoria de funcionamento das urnas eletrônicas em condições normais de uso (Módulo Votação); o Verificador Pré/Pós-Eleição (VPP) e o Verificador de Integridade e Autenticidade de sistemas eleitorais (AVPART), utilizados para a verificação de resumos digitais (hashes) e assinatura digital nas urnas eletrônicas;
- Ampliação da quantidade de participantes que podem ser admitidos (grupos ou individuais), passando de 10 para 15;
- Ampliação do prazo para os interessados em participar inspecionarem os códigos-fonte dos sistemas eleitorais para duas semanas, com o pagamento de passagens e diárias;
- Possibilidade de extensão excepcional por mais um dia, caso seja constatada a necessidade de dar continuidade à execução dos planos de testes, totalizando, dessa forma 6 dias. Extensão de prazo solicitada e deferida pela equipe de investigadores da Polícia Federal.

Em decorrência das inovações implementadas, visando ampliar a colaboração da sociedade no desenvolvimento dos sistemas eleitorais, essa edição contou com a participação recorde de investigadores e planos de testes submetidos. Ao total, foram 26 investigadoras e investigadores que buscaram executar 29 planos de ataque aos equipamentos e sistemas que serão usados nas Eleições Gerais de 2022.

O TPS 2021 contou, ainda, com uma ampla cobertura nas mídias sociais e no canal oficial da Justiça Eleitoral no YouTube, possibilitando o acompanhamento do evento por quem não estivesse nas dependências do TSE.

O relatório a seguir é o primeiro apresentado pela Comissão Reguladora do TPS 2021, com a descrição dos planos de testes executados, os achados durante essa execução e avaliação técnica preliminar. Após o teste de confirmação, com a validação das melhorias implementadas em decorrência dos achados dessa edição, será apresentado um novo relatório técnico e, ao final, o compêndio do TPS 2021, com todos dados e informações do evento.

SUMÁRIO DOS PLANOS DE TESTES APROVADOS

Id	Nome	Investigadores	Situação
1	Invasão ao JE-Connect	Fellipe Ribeiro da Silva Abib, Caio Henrique de Aquino Vicente, Charles William Biesseki e Alan Papafanurakis Heleno.	Encerrado sem achados.
2	Rastrear a ordem de votação dentro do BU	Tiago Silva Mazzante e Felipe Fonteles Belo	Encerrado sem achados
3	Verificação do comportamento do parâmetro urna: mcriptografar	André Luiz Matos	Encerrado COM achado
4	Invasão Leiga: Soldadinho-do-Araripe	Gabriel Leonardo Sena dos Santos	Encerrado sem achados
5	Modificação do BU e RDV para teste de validação de assinatura	Marcos Roberto dos Santos, Adroaldo Leão Souto Júnior, Gabriel Sordi Damo, Juliano Ribeiro Poli e Vinícius Borges Fortes.	Encerrado sem achados
6	Keylogger não intrusivo	Marcos Roberto dos Santos, Adroaldo Leão Souto Júnior, Gabriel Sordi Damo, Juliano Ribeiro Poli e Vinícius Borges Fortes.	Encerrado COM achado
7	Recuperação de dados sensíveis enviados via método GET	Lúcio Santos de Sá	Encerrado sem achados
8	Executar JEC em máquina com firmware de componente não proprietário e não assinado.	Lúcio Santos de Sá	Encerrado sem achados
9	Identificar teclas pressionadas através do retorno tátil sonoro do teclado da Urna Eletrônica	Lúcio Santos de Sá	Não executado
10	Execução de ataques de agente autorizado com o uso do JEC	Lúcio Santos de Sá	Não executado
11	Alteração de informações da tabela de correspondência	Paulo César Herrmann Wanner, Ivo de Carvalho Peixinho e Galileo Batista de Sousa	Encerrado sem achados
12	Extração de dados e configurações do Kit JE Connect	Paulo César Herrmann Wanner, Ivo de Carvalho Peixinho e Galileo Batista de Sousa	Encerrado COM achado
13	Captura, análise e decodificação de sinais elétricos colaterais nas portas externas	Anderson Cunha (colaborativo)	Encerrado sem achados

14	Registro digital do voto e ordem de votação: possível quebra de sigilo	Lorenna Rodrigues Tredezzini	Encerrado sem achados
15	GEDAI-UE, SAVP Sorteio e Votação e Módulo	Felipe de Lima e Lima	Não executado
16	Segurança do JE Connect e do Firefox	Felipe de Lima e Lima	Encerrado COM achados
17	Segurança do RecArquivos e InfoArquivos	Felipe de Lima e Lima	Não executado
18	Sistot, Transportador e Transportador Backend	Felipe de Lima e Lima	Não executado
19	MSD, Bios, Bootloader, UENUX, APPs e Dados & Processo de compilação do UENUX	Felipe de Lima e Lima	Encerrado sem achados
20	Violar o sigilo do voto	Ian Martinez Zimmermann Carlos Alberto da Silva	Encerrado COM achados
22	Captura, análise e decodificação de sinais elétricos colaterais nas portas externas	Nayara Sávia Alves Alencar (colaborativo)	Encerrado sem achados
23	Análise e decodificação de sinais eletromagnéticos a distância	Lucas Pavão de Carvalho Xavier	Não executado
24	Captura, análise e decodificação de sinais elétricos colaterais nas portas externas	Lucas Pavão de Carvalho Xavier (colaborativo)	Encerrado sem achados
26	Indução eletromagnética	Lucas Pavão de Carvalho Xavier	Não executado
27	Inserção de serviço Windows não autorizado no SIS	Lucas Pavão de Carvalho Xavier	Encerrado sem achados
29	Alteração do teor dos arquivos na mídia de preparação – pós GEDAI-UE	Lucas Pavão de Carvalho Xavier	Encerrado sem achados
30	Sistema / Programa Transportador de Arquivos (JE-Connect)	Rodrigo Cardoso Silva	Encerrado sem achados
31	Vitruviano	Kennedy Antônio Vasconcelos Ferreira Júnior	Encerrado sem achados
32	Captura, análise e decodificação de sinais elétricos colaterais nas portas externas	Lúcio Santos de Sá (colaborativo)	Encerrado sem achados

Os planos de números 21, 25 e 28 não foram aprovados e consequentemente não fizeram parte do TPS.

PLANO DE TESTE 1: INVASÃO AO JE-CONNECT

Investigadores: Fellipe Ribeiro da Silva Abib, Caio Henrique de Aquino Vicente, Charles William Biesseki e Alan Papafanurakis Heleno.

Objetivo: Desmontar o JE Connect para extrair as informações da VPN e utilizar essa conexão fora do sistema JE Connect. Assim seria possível se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.

Etapas Propostas:

1. Inicialização do JEConnect numa máquina virtual
2. Extração do dump de memória
3. Extração da chave de VPN

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi facilitado o ataque coma a não utilização de lacres físicos, abertura da urna e fornecimento de documentação de hardware e esquemas elétricos. Não obtiveram sucesso pelo acionamento do timeout do Hardware de Segurança da placa-mãe, pios a urna se desligou ao não detectar um sistema operacional autêntico. No caso dos sinais capturados, a criptografia de canal impediu que o sinal fosse decodificado.

Considerações técnicas: Os investigadores conseguiram captar um sinal nas portas USB traseiras semelhantes ao sinal encontrado na interface USB do Teclado do Terminal do Eleitor. Há a hipótese de que o sinal possa ser replicado ou decodificado, mas os investigadores não conseguiram êxito. Outras tentativas foram feitas em trocar o sistema operacional a ser executado.

PLANO DE TESTE 2: RASTREAR A ORDEM DE VOTAÇÃO DENTRO DO BU

Investigadores: Tiago Silva Mazzante e Felipe Fonteles Belo

Objetivo: Abrir o Boletim de Urna, depois de uma eleição, para identificar os votos com a intenção quebrar o sigilo.

Etapas Propostas:

Identificação do funcionamento da geração do BU

Entendimento da função randômica e sua efetivação

Identificação de padrões a fim de uma possível réplica em outros cenários

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado arquivo de configuração (parâmetros de urna - PU) ajustado para que a urna gerasse o BU sem criptografia e, com isso, fosse possível analisar o seu conteúdo.

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de identificar a sequência de votação a partir do BU.

PLANO DE TESTE 3: VERIFICAÇÃO DO COMPORTAMENTO DO PARÂMETRO URNA: MCRIPTOGRAFAR

Investigadores: André Luiz de Matos

Objetivo: O parâmetro default para a configuração da urna mcriptografar (True) pode ser alterado internamente para (False) ou outros por usuário interno antes de procedimentos de lacração, neste sentido entende-se por uma visão de alto nível que a urna emitirá um BU sem as devidas assinaturas e criptografias. Caso isso ocorra faz-se necessário observar o comportamento das outras camadas de segurança impedindo o prosseguimento de geração de arquivos RDV e BU para transporte e ou impedimento de transporte do arquivo sem as devidas criptografias. Verificação de configurações do transportador P_TB_CONFIGURA_TRANSPORTADOR(REC) a fim de avaliar possível aceitação de mídias sem criptografia.

Etapas Propostas: Simular alteração intencional do parâmetro mcriptografar de (True) par (False) ou outra aceita e seguir com as demais rotinas de compilação "lacração", geração de mídias e carga inicial em urna, simular votação e verificar possível geração de RDV e BU sem assinaturas e criptografias.

Verificação de configuração do transportador P_TB_CONFIGURA_TRANSPORTADOR(REC).

Resultado: Plano de teste executado com achado: recebimento de Boletim de Urna sem criptografia.

Barreiras derrubadas: Foi disponibilizado arquivo de configuração (parâmetros de urna - PU) ajustado para que a urna gerasse o BU sem criptografia e, com isso, fosse possível analisar o seu conteúdo, assim como proceder com o transporte do arquivo.

Considerações técnicas: No dia 22/11/2021, houve o início do teste "Verificação do comportamento do paramento da urna: mcriptografar" realizado pelo investigador André Luiz de Matos e acompanhado pelo observador José Cassimiro Júnior. O arquivo de configuração gerado pelo GEDAI-UE é assinado e interpretado pela Urna Eletrônica – UE. Ele possui vários parâmetros, e dentre eles, o MCRIPTOGRAFAR, com as opções true ou false, com o objetivo de informar se os boletins de urna serão gerados de forma criptografada ou não. Por padrão, todos os BU são gerados de forma criptografada (opção true). O parâmetro MCRIPTOGRAFAR existe para permitir a geração de BU sem criptografia exclusivamente para eleições comunitárias, de modo que as entidades que solicitaram o empréstimo das urnas possam conduzir a sua própria totalização da eleição. Devido à previsão no edital da impossibilidade de alteração do código fonte dos sistemas (edital do TPS 2021), o investigador solicitou a geração de um novo arquivo de configuração do GEDAI-UE, com parâmetro o mcriptografar definido com a opção false. O pedido foi aprovado pela comissão reguladora. Com o auxílio da equipe da SEVIN, houve alteração do parâmetro MCRIPTOGRAFAR para false e uma nova assinatura do arquivo de configuração do GEDAI-UE foi gerada para possibilitar a validação correta na UE. Após esse procedimento, o investigador realizou uma nova votação na urna eletrônica com o parâmetro MCRIPTOGRAFAR alterado para false, o que possibilitou a geração dos boletins de urna sem criptografia, porém, com assinatura digital. Após a aprovação do pedido de instalação do editor de ASN.1 pela comissão reguladora, o investigador alterou o número do candidato no qual havia votado, persistiu a alteração no BU e realizou a respectiva transmissão dos arquivos modificados por meio do Transportador no kit JE-Connect. Após a tentativa de leitura desse arquivo de BU adulterado, houve a correta apresentação da mensagem de erro na assinatura digital do arquivo e, consequentemente, não foi habilitada a sua transmissão para o Rec-Arquivos-Urna. Após esse teste, o investigador realizou a alteração do BU para o seu estado inicial, isto é, o mesmo gerado pela UE (sem criptografia e alteração) e realizou a leitura desse arquivo pelo Transportador, que por sua vez, não acusou nenhum erro de assinatura digital. Após esse procedimento, houve a transmissão desse BU pelo Transportador e sucesso no recebimento e validação no Rec-Arquivos-Urna, apesar da ausência da criptografia no BU. Foi constatado, portanto, que o RecAquivos recebeu sem erro BU em claro, ou seja, sem criptografia. Contudo o sistema corretamente não permitiu o envio tampouco o recebimento de arquivo alterado e consequentemente com assinatura inválida, ainda que sem criptografia. A Seção de Totalização e Divulgação de Resultados reavaliará o comportamento do sistema quanto ao recebimento de BUs sem criptografia.

PLANO DE TESTE 4: INVASÃO LEIGA: SOLDADINHO-DO-ARARIPE

Investigadores: Gabriel Leonardo de Sena Santos

Objetivo: O ataque seria ao software da urna, alterando os dados SCUE e simulando uma pane.

Aconteceria da metade para o fim da votação, ajustando o ADH e programando o horário para instabilidade (por exemplo,14:30). Então utilizaria o RED para recuperar os dados da urna, esse já estaria modificado com a mesma quantidade de votos dos eleitores que já votaram, porém, esses votos iriam para candidatos diferentes dos escolhidos pelo eleitor.

Etapas Propostas:

1. Simular votação em uma UE previamente preparada
2. Executar contingência, substituindo UE por UE de contingência previamente preparada
3. Na urna original substituída, executar contingência de FV
4. Seguir votação nas 2 urnas

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Nenhum procedimento de controle relativo à contingência de urna ou recuperação de resultados foi aplicado, sendo possível a livre execução do software da urna.

Considerações técnicas: Nenhum achado. O investigador não foi capaz de alterar qualquer dado na urna.

PLANO DE TESTE 5: MODIFICAÇÃO DO BU E RDV PARA TESTE DE VALIDAÇÃO DE ASSINATURA

Investigadores: Marcos Roberto dos Santos, Adroaldo Leão Souto Júnior, Gabriel Sordi Damo, Juliano Ribeiro Poli e Vinícius Borges Fortes.

Objetivo: Alteração do arquivo que contém os votos gerado pela urna e teste de envio com nova assinatura gerada com chave fake

Etapas Propostas:

1. Geração de mídias e carga da UE

2. Votação de 5 eleitores

3. Impressão de BU encriptado

4. Alteração da configuração do GEDAI-UE para gerar BU sem encriptação

5. Geração de mídias e nova carga da UE

6. Votação de 5 eleitores

7. Impressão de BU sem encriptação

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado arquivo de configuração (parâmetros de urna - PU) ajustado para que a urna gerasse o BU sem criptografia e, com isso, fosse possível analisar e modificar o seu conteúdo.

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de alterar o resultado da votação no BU.

PLANO DE TESTE 6: KEYLOGGER NÃO INTRUSIVO

Investigadores: Marcos Roberto dos Santos, Adroaldo Leão Souto Júnior, Gabriel Sordi Damo, Juliano Ribeiro Poli e Vinícius Borges Fortes.

Objetivo: Será criado um invólucro (cópia perfeita, no formato da UE, porém com dimensões levemente maiores) através de uma impressora 3D e cortadora laser, o qual terá por finalidade sobrepor toda a urna, salvo sua parte traseira, inclusive sobrepondo o teclado com um protótipo falso. Tendo por objetivo inicial registrar todos os cliques efetuados na urna em um microchip, relacionando os dados com data e hora. O microchip possuirá um módulo bluetooth o qual transmitirá os dados registrados em tempo real para o atacante, além de armazená-los. A efetividade deste ataque consiste em conseguir associar o voto com o eleitor, quebrando, assim, o sigilo do voto. Para isso um simples observador (poderia ser um vídeo), pode registrar o momento do voto de qualquer pessoa, relacionando a hora e voto. Para este ataque ser indetectável, é necessário que dois atacantes votem na mesma seção eleitoral, um para instalar o invólucro e outro para retirá-lo.

Etapas Propostas:

1. Instalação o dispositivo no painel frontal da UE

2. Ajustes na sensibilidade das teclas do dispositivo

3. Teste de conectividade do wi-fi roteado pelo smartphone

4. Envio dos dados em tempo real para banco na nuvem

5. Visualização em dispositivo externo para monitoramento das teclas digitadas na UE

6. Os testes foram realizados com fonte elétrica, bem como com bateria acoplada a um Raspberry Pi

Resultado: Plano de teste executado com achado: a UE 2015 não possui nenhum dispositivo capaz de identificar um invólucro sobreposto à parte frontal, o que possibilitou a instalação de um dispositivo de monitoramento de pressão de teclas (keylogger não intrusivo)

Soluções sugeridas:

1. Redução da altura da cabine de votação permitindo que o mesário tenha visão parcial do eleitor, evitando que trazer peças do invólucro escondidas sob sua roupa

2. Instalação de um sensor de proximidade em pontos estratégicos da UE, como o teclado, para detectar elementos próximos, informando por meio de leds o terminal do mesário 3. Treinamento de mesários para verificação da UE a cada X eleitores.

Barreiras derrubadas: O ambiente simulado de uma seção eleitoral não foi simulado, ou seja, o grupo de investigadores fez os procedimentos com um protótipo sobre a urna e uma cabina de votação. Não foi possível avaliar a facilidade com que um eventual atacante pudesse montar e desmontar o aparato sem que fosse detectado. Contudo, o painel falso mostrou-se como uma abordagem interessante, para a qual deve ser verificado se há soluções para mitigá-la, tanto procedimentais quanto tecnológicas.

Considerações técnicas: Os investigadores utilizaram um painel frontal falso, fabricado em impressora 3D em várias peças, que deve ser montado por um eleitor/atacante que se aproveitará da privacidade na cabina de votação para instalar o dispositivo. Outro eleitor/atacante seria o responsável por desmontar e retirar o dispositivo da urna antes do final da votação para não ser detectado. O dispositivo deve deixar o display do Terminal do Eleitor à mostra e simular, da forma mais perfeita possível, um teclado e o restante do painel frontal, de modo a diminuir as chances do dispositivo ser detectado. Cada tecla do teclado do dispositivo tem um sensor ou chave que é pressionada quando a tecla falsa está sobre a tecla verdadeira, possibilitando que cada tecla seja capturada assim que pressionada pelo eleitor. A forma interna de gravação e transmissão podem ter abordagens diferentes, mas que podem formar um certo volume que aumente de alguma forma o painel frontal, aumentando a

probabilidade de alguém perceber o dispositivo falso. As soluções apresentadas serão avaliadas, mas a mais adequada, a princípio, seria a diminuição da cabina eleitoral.

PLANO DE TESTE 7: RECUPERAÇÃO DE DADOS SENSÍVEIS ENVIADOS VIA MÉTODO GET

Investigadores: Lúcio Santo de Sá

Objetivo: O objetivo do teste proposto será utilizar dos conhecimentos adquiridos durante a inspeção dos códigos fontes, para recuperar dados sensíveis que estão atualmente sendo transmitidos via método GET, que muitas vezes são armazenados em locais do servidor ou proxy sem nenhum tipo de criptografia aplicada.

Etapas Propostas:

1. Tentar Recuperar os dados sensíveis através dos locais mencionados
2. Observar se o JE Connect também realiza conexão, permitindo que os dados sejam recuperados por um agente malicioso com acesso físico à mídia Resultado: Plano de teste executado sem achados.

Resultados: Plano executado sem achados.

Barreiras derrubadas: Fornecimento do PIN;

Considerações técnicas: O teste não foi realizado, pois havia dependência com sucesso na realização do teste nº 8;

PLANO DE TESTE 8: EXECUTAR JE CONNECT EM MÁQUINA COM FIRMWARE DE COMPONENTE NÃO PROPRIETÁRIO E NÃO ASSINADO

Investigadores: Lúcio Santos de Sá

Objetivo: Testar a possibilidade de se iniciar o JE Connect (JEC) em máquina contendo componentes com firmware não proprietário e não assinado instalado. Sem a validação das assinaturas dos componentes como BIOS, HD e GPU um agente malicioso com acesso prévio à máquina que será utilizado o JEC poderia fazer uso de um UEFI RootKit (por exemplo) para ter acesso ao sistema UNIX da mídia, já que ela faz uso indiscriminado destes componentes e suas APIs de alto nível.

Etapas Propostas:

1. Votação simulada e encerrando a Urna gravando o resultado em uma mídia de resultados
2. Exploração do JEC, gravando os logs numa pasta FAT

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Fornecimento do PIN;

Considerações técnicas: Não conseguiu superar a barreira do JEC Connect que impede sua execução em máquina virtual.

PLANO DE TESTE 9: IDENTIFICAR TECLAS PRESSIONADAS ATRAVÉS DO RETORNO TÁTIL SONORO DO TECLADO DA URNA ELETRÔNICA

Investigadores: Lúcio Santos de Sá

Objetivo: Utilizando-se do retorno tátil sonoro do teclado presente nos modelos da Urna Eletrônica, utilizar de modelo de predição previamente configurado para identificar diferentes pressionamentos de teclas, e por consequência, quebrando o sigilo do voto.

Etapas Propostas:

1. Realizar o treino do modelo de predição;
2. Gravar o pressionamento de teclas;
3. Realizar o reconhecimento do voto.

Resultado: Não executado.

Barreiras derrubadas: N/A.

Considerações técnicas: N/A.

PLANO DE TESTE 10: EXECUÇÃO DE ATAQUES DE AGENTE AUTORIZADO COM O USO DO JE CONNECT

Investigadores: Lúcio Santos de Sá

Objetivo: Após a análise de código, foi observado que alguns dos sistemas de uso autenticado do JE Connect possuíam a proteção contra Cross Site Scripting desabilitada. Sendo assim, o objetivo deste teste é realizar ataques aos servidores como um agente autenticado. Dentre os métodos, incluem-se: CSRF, Race Condition, HTTP Smuggling e Cache Poisoning.

Etapas Propostas:

1. Inserir mídia do JE Connect;
2. Se autenticar ao JE Connect;
3. Realizar os ataques descritos.

Resultado: Não executado.

Barreiras derrubadas: Fornecimento do PIN;

Considerações técnicas: Não conseguiu superar a barreira do JEC Connect que impede sua execução em máquina virtual.

PLANO DE TESTE 11: ALTERAÇÃO DE INFORMAÇÕES DA TABELA DE CORRESPONDÊNCIA

Investigadores: Paulo César Herrmann Wanner, Ivo de Carvalho Peixinho e Galileo Batista de Sousa

Objetivo: O teste visa verificar a possibilidade de alteração maliciosa dos dados de correspondência das urnas eletrônicas e o comportamento do sistema de totalização quando dados de votação são recebidos sem as informações de correspondência necessárias.

A alteração de dados de correspondência referentes a inseminação das urnas eletrônicas deve ser detectada e a falta dessas informações deve gerar um alerta de segurança, visto que irão impactar no sistema de totalização futuramente. O sistema de votação brasileiro deve detectar urnas sem dados de correspondência antes do início do período de votação e sanar tais falhas evitando um impacto futuro do processo de votação.

Etapas Propostas:

1. Inseminar uma urna eletrônica com dados válidos
2. Alterar os dados da tabela de correspondência do cartão de memória utilizado na inseminação

3. Utilizar o GEDAI-UE para ler a tabela de correspondência

4. Verificar se o GEDAI-UE carrega as informações e as encaminha para o Sistema de Totalização

5. Verificar como o Sistema de Totalização se comporta ao receber os arquivos de votação de Urnas sem correspondência na tabela de correspondência de suas bases de dados

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado amplo acesso às mídias das urnas, assim como do disco rígido da estação de trabalho onde se encontrava o Gedai-UE.

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de manipular a tabela de correspondências, tanto na urna quanto no Gedai-UE.

PLANO DE TESTE 12: EXTRAÇÃO DE DADOS E CONFIGURAÇÕES DO KIT JE CONNECT

Investigadores: César Herrmann Wanner, Ivo de Carvalho Peixinho e Galileo Batista de Sousa

Objetivo: O teste visa verificar a possibilidade de extração de informações do Kit JE Connect que permitam acessar a rede do TSE através de uma VPN. Obtendo-se acesso a rede interna, visa-se encontrar vulnerabilidades no sistema de recebimento de arquivos da urna eletrônica a partir de técnicas fuzzing e acesso direto ao banco de dados do totalizador e as suas rotinas.

Etapas Propostas:

1. Realizar imagem da mídia JE Connect

2. Inicialização a mídia JE Connect em um ambiente virtualizado para realizar um dump de memória

3. Montagem dos dados existente no sistema de arquivos a fim de identificar credenciais e configuração da VPN

4. Caso seja possível obter tais informações, estabelecer uma conexão via VPN e testar o recebimento de arquivos utilizando técnicas fuzzing

Resultado: Teste executado com achados.

Barreiras derrubadas: Fornecimento do PIN; Fornecimento de senha de oficialização do KIT (para possibilitar o prosseguimento dos trabalhos no sábado);

Chegaram a capturar o certificado de conexão usado pelo JEConnect para estabelecer conexão com a rede da Justiça Eleitoral e se conectaram à rede do TSE com esse certificado a partir de ambiente sem os controles do Je-Connect. O Firewall PFSense inibiu movimentação lateral Firewall de datacenter inibiu acesso a servidores; Balanceador inibiu acesso a bancos de dados e servidores; Web Application Firewall inibiu explorações adicionais (Command Injection).

Considerações técnicas: A equipe da Polícia Federal obteve achados importantes para a Justiça Eleitoral. Em que pese não ter havido quebra de sigilo ou alteração de destinação do voto, a equipe utilizou técnicas avançadas de engenharia reversa, convertendo programas executáveis para linguagem Assembler, de modo a burlar controles implementados no aplicativo JE-Connect. Utilizando senha do aplicativo JE-Connect fornecida pelo TSE (de modo a simular um ataque interno) e as estratégias de engenharia reversa, obtiveram a chave mestra utilizada pelo sistema operacional Linux para criptografia de disco (LUKS). A descoberta da chave mestra do Linux foi utilizada para leitura do disco de sistema e decriptografia da primeira partição do JE-Connect, a partição BOOT (disco contendo arquivos de inicialização do sistema). Ainda usando engenharia reversa, encontraram nessa primeira partição do Kit JE-Connect a chave para decriptação da segunda partição do Kit, a partição ROOT (disco contendo o sistema). Por meio de buscas na partição ROOT e executando as aplicações que se conectavam à rede da Justiça Eleitoral, encontraram a chave então configurada para estabelecer conexão VPN com a rede local do TPS, mas sem ultrapassar as barreiras de segurança entre a rede local e os servidores que hospedam os sistemas eleitorais. Registramos que o principal achado foi conseguir extrair do Kit JE-Connect o certificado para conexão com a rede do TPS e utilizá-lo fora do Kit. A conexão com a rede do TPS já seria possível mediante a utilização da senha de acesso requerida pela Polícia Federal e fornecida pelo TSE. Por fim, conseguiram executar o sistema Transportador fora do ambiente do JE-Connect.

PLANO DE TESTE 13: CAPTURA, ANÁLISE E DECODIFICAÇÃO DE SINAIS ELÉTRICOS COLATERAIS NAS PORTAS EXTERNAS

Investigadores: Anderson Cunha (Executado em conjunto com os investigadores Nayara Sávia Ayres Alencar, Lúcio de Santos Sá, Lucas Pavão)

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de capturar, armazenar e decodificar possíveis vazamentos de ruídos elétricos decodificáveis de diferentes barramentos que não tenham sido contidos por filtros passivos existentes nas portas.

Etapas Propostas:

1. Medição de sinais elétricos das portas externas por meio de instrumentos durante a digitação por parte do eleitor
2. Uso de dispositivos para captura, amplificação e filtragem desses sinais
3. Uso de software para análise e processamento digital

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi facilitado o ataque com a não utilização de lacres físicos, abertura da urna e fornecimento de documentação de hardware e esquemas elétricos. Não obtiveram sucesso pelo acionamento do timeout do Hardware de Segurança da placa-mãe, pios a urna desligou ao não detectar um sistema operacional autêntico. No caso dos sinais capturados, a criptografia de canal impediu que o sinal fosse decodificado.

Considerações técnicas: Os investigadores conseguiram captar um sinal nas portas USB traseiras semelhantes ao sinal encontrado na interface USB do Teclado do Terminal do Eleitor. Há a hipótese de que o sinal possa ser replicado ou decodificado, mas os investigadores não conseguiram êxito. Outras tentativas foram feitas em trocar o sistema operacional a ser executado.

PLANO DE TESTE 14: REGISTRO DIGITAL DO VOTO E ORDEM DE VOTAÇÃO POSSÍVEL QUEBRA DE SIGILO

Investigadora: Lorenna Tredezini

Objetivo: Realização de uma votação simulada com 15 eleitores fictícios, na qual os 10 primeiros eleitores votam nominalmente no mesmo candidato a vereador e os 5 primeiros votam no candidato a prefeito com o menor numeral (ex. 11) e os 5 seguintes no segundo maior número (ex. 12), sendo que os 5 subsequentes votam normalmente em candidatos aleatórios.

O que garante o sigilo do voto é o tipo do voto (voto de legenda, nominal, branco ou nulo) e a digitação do eleitor (número do candidato), de modo que estes são armazenados de forma lexicográfica, no registro digital do voto – RDV. Assim, uma vez estabelecido o formato ASN.1 para registro e gravação desses dados, o sigilo constitucionalmente imposto estaria garantido.

Os valores ASN.1 são codificados em três campos. Essa estrutura geral é válida para todos os tipos, sejam estes primitivos ou construídos.

Entretanto, em uma lista ordenada por, hipoteticamente, valores iguais (mesmo tipo de voto, p. ex., voto nominal, seguido de voto em um determinado vereador, p. ex. 11.101, com número sucessivo para um eventual candidato a prefeito, em que os 10 primeiros eleitores aptos de uma seção assim votariam de forma pré combinada), questiona-se se os votos seriam lidos e registrados na mesma ordem no RDV, porquanto o mecanismo utilizado para o registro do voto seria a ordem natural da votação já que ausente sequência de valores de tipos diferentes.

Etapas Propostas:

1. Acesso ao GEDAI-UE e geração das mídias de carga, votação e resultado
2. Carga na Urna Eletrônica
3. Realizar votação combinada de determinado número de eleitores iniciais da seção eleitoral e dos demais de maneira aleatória
4. Visualizar o arquivo do RDV para verificar se alguma forma coincide a ordem

de votação

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado amplo acesso ao conteúdo das mídias de resultado das urnas.

Considerações técnicas: Nenhum achado. A investigadora não foi capaz de identificar a sequência de votação a partir do RDV.

PLANO DE TESTE 15: GEDAI-UE, SAVP-SORTEIO E VOTAÇÃO E MÓDULO

Investigadores: Felipe de Lima e Lima

Objetivo: Garantir a integridade e segurança do GEDAI-UU e outros sistemas pela Módulo e outros subsistemas de segurança depois de instalado numa máquina Windows, impendido que um agente não autorizado modifique ou interfira com os sistemas.

Etapas Propostas:

1. Verificar a integridade e resistência dos sistemas de segurança: 1. **Segurança do OS** – Verificar que após a instalação dos módulos de segurança sobre o Windows com os 4 perfis

configurados, não é possível que um agente consiga o acesso do perfil de Suporte (Admin) sem estar devidamente autorizado.

2. **Ataque de Dump de Memória** – Verificar que o Windows e os módulos de segurança resistam a revelar informações sensíveis quando a memória RAM do computador é lida pelo atacante.

Resultado: Não executado.

Barreiras derrubadas: Foi disponibilizado amplo acesso ao computador SIS onde os sistemas estavam instalados, assim como acesso ao seu disco rígido e possiblidade de inicialização de outro sistema operacional no computador (Kali Linux).

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de manipular os aplicativos desktop Gedai-UE, Sorteio e Votação.

PLANO DE TESTE 16: SEGURANÇA DO JE-CONNECT E DO FIREFOX

Investigadores: Felipe de Lima e Lima

Objetivo: Garantir a integridade e segurança do JE Connect com o Firefox em cenários e falha e cenários de ataque diversos pois esses são executados em ambientes fora do controle do TSE.

Etapas Propostas:

- Verificar que o JE Connect é resistente a falhas externas diversas:
  - **Falha de energia** - Iniciar o computador com o JE Connect e retirar a energia do computador para verificar se o JE Connect executa normalmente na próxima inicialização.
  - **Falha de conexão** – Iniciar a transmissão do arquivo do ponto de transmissão e verificar se o Je Connect trabalha corretamente com o Transportador para garantir que não haja nenhum problema caso haja interrupção na transmissão.
- Verificar a integridade do JE Connect contra atacantes:
  - **Análise do Arquivo de Sistemas** – Colocar o drive do JE Connect em outro computador sem o token, utilizar um outro OS (Linux ou Windows) para analise o JE Connect e tentar comprometer as suas defesas.

- **Robustez do Firefox** – Verificar se o Firefox instalado no JE Connect foi corretamente instalado e protegido.

Resultado: Plano de teste executado com 3 achados:

- Achado 1: Usuário chegou ao Firewall do TSE

  Passos: a) Abrir o navegador no JE Connect

  b) Utilizar o atalho "/" e "SHIFT+F3"

  c) Copiar o IP do Gateway para a janela de busca

  d) Selecionar tudo com o mouse

  e) Arrastar para a janela do Firefox

  Solução sugerida: Desabilitar o atalho "/" e "SHIFT+F3"

- Achado 2:
  - Usuário com a senha de acesso faz login no JE Connect;
  - aciona e segura o botão esquerdo do mouse;
  - aciona o botão direito do mouse sobre a barra de tarefas;
  - então o S.O. mostra o menu de contexto.

  Solução sugerida: Bloquear o botão direito mesmo com o esquerdo acionado.

- Achado 3:
  - Usuário conecta o JE Connect com a VPN e abre a janela do Firefox;
  - desconecta da VPN;
  - muda o cabo de conexão para outro ponto (com um roteador externo) e conecta nesse roteador sem a VPN;
  - então consegue acessar a Internet ou qualquer outro computador na rede do roteador, utilizando o drag and drop do Firefox.

  Nenhuma solução sugerida.

Barreiras derrubadas: Fornecimento do PIN;

Chegou a usar teclas de atalho do navegador FireFox para tentar explorar eventuais vulnerabilidades na rede. Barreiras de segurança que os detiveram: Firewall de internet do TSE.

Considerações técnicas:

Achado 1: Na execução do teste proposto de Robustez do Firefox, que é o navegador instalado no JE Connect, foi detectado que a tecla "\" do teclado numérico e o conjunto de teclas SHIFT+F3, que aciona a funcionalidade "Quick Find" do navegador, não estão bloqueadas. Ao acionar estas teclas, o navegador apresenta uma barra de pesquisa, onde o usuário digita um texto que pode ser arrastado para a janela ativa do navegador, resultando na apresentação desta busca na rede. Como os elementos da rede são controlados por credenciais (usuário e senha) ou não respondem a esta pesquisa, este achado fica restrito à tela do navegador.

Achado 2: O conjunto de teclas "botão direito e esquerdo do mouse" quando acionadas sobre a barra de tarefas, não estão bloqueadas, e o resultado é a apresentação do menu de contexto.

Achado 3: O pressuposto do uso do JEConnect é a existência de uma conexão à internet conectada ao computador hospedeiro. Assim quando a conexão VPN não está ativa o computador está ligado à rede local do ambiente onde está instalado. A navegação só foi possível pelo uso do procedimento detalhado no ACHADO 1.

PLANO DE TESTE 17: SEGURANÇA DO REC-ARQUIVOS E INFO-ARQUIVOS

Investigadores: Felipe de Lima e Lima

Objetivo: Garantir a integridade e a segurança do Info-Arquivos e Rec-Arquivos nas suas execuções. Verificar se Rec-Arquivos está devidamente protegendo todos os dados da urna quando realizar a transmissão para o TSE.

Etapas Propostas:

- Verificar que o REC-Arquivos é resistente a falhas externas diversas:

  1. **Falha de energia** – Desligar a energia da máquina que estiver processando o recebimento do REC-Arquivos no momento da transmissão para garantir que não danos aos BUs ou outros arquivos antes de irem para DB do TSE.

2. **Falha de conexão** – Iniciar a transmissão do arquivo do ponto de transmissão e verificar se o REC-Arquivos trabalha corretamente com o Transportador para garantir que não haja nenhum problema quando a conexão é interrompida.

- Verificar a integridade e resistência do REC-Arquivos contra atacantes:

  1. Segurança do processo de Build – Substituir a biblioteca da CEPESC por outra com hash diferente ou inválido para garantir que não será incluída nenhum código malicioso no momento do build da aplicação por agentes não autorizados.

  2. Ataque de Interceptação – Verificar que o REC-Arquivos recusa ou não aceita pacotes que não foram enviados por uma urna válida do TSE ou que foram alterados.

Resultado: Não executado.

Barreiras derrubadas: Não executado

Considerações técnicas: Não executado. O investigador Felipe de Lima e Lima apresentou cinco planos de testes, dentre eles, o "Segurança do REC Arquivos e INFO Arquivos". Conforme o relatório do observador, não houve registro de execução desse plano, pois houve a priorização e execução dos demais.

PLANO DE TESTE 18: SISTOT, TRANSPORTADOR E TRANSPORTADOR BACKEND

Investigadores: Felipe de Lima e Lima

Objetivo: Verificar se o Transportador está protegendo devidamente todos os dados da urna quando realizar a transmissão para o RECArquivos. O Transportador tem alta criticidade pela sua importância no momento da transmissão dos dados para o TSE.

Por isso, deve ser resiliente caso tentem interceptar os pacotes (testar de cifragem e Man-in-Middle) e em casos de falhas externas (falta de luz ou perda de conexão).

Além disso, o Transportador é executado fora do ambiente do TSE em máquinas externas que podem ter a sua segurança comprometida que estão mais suscetíveis a agentes maliciosos.

Etapas Propostas:

- Verificar que o Transportador é resistente a falhas externas diversas:

    1. **Falha de energia** – Desligar a energia da máquina no momento da transmissão para garantir que não danos aos BUs ou outros arquivos antes de irem para o TSE.

    2. **Falha de conexão** – Iniciar a transmissão do arquivo do ponto de transmissão e verificar se o REC-Arquivos trabalha corretamente com o Transportador para garantir que não haja nenhum problema quando a conexão é interrompida.

- Verificar a integridade e resistência do Transportador contra atacantes:

    1. **Segurança do processo de Build** – Substituir a biblioteca da CEPESC por outra com hash diferente ou inválido para garantir que não será incluída nenhum código malicioso no momento do build da aplicação por agentes não autorizados.

    2. **Ataque de Decifragem** – Verificar que o Transportador cifra os dados para evitar leitura de agentes não autorizados.

    3. **Ataque de Interceptação** – Verificar que o Transportador é resistente a um ataque Man-in-Middle em caso de agentes não autorizados estarem tentando interceptar a conexão.

    4. **Ataque de configuração maliciosa** – Verificar que o Transportador ao ser executado de forma errada propositadamente (por linha de comando ou por chamada de outro programa) não compromete os BUs e outros dados sensíveis.

    5. **Ataque de Dump de Memória** – Verificar que o Transportador ao ser executado num possível computador comprometido é resistente a revelar informações sensíveis quando a memória RAM do computador é lidar pelo atacante

Resultado: Não executado.

Barreiras derrubadas: Não executado.

Considerações técnicas: Não executado. O investigador Felipe de Lima e Lima apresentou cinco planos de testes, dentre eles, o “Sistot, Transportador e Transportador Backend". Conforme o relatório do observador, não houve registro de execução desse plano, pois houve a priorização e execução dos demais.

PLANO DE TESTE 19: MSD, BIOS, BOOTLOADER, UENUX, APPS E DADOS & PROCESSOS DE COMPILAÇÃO DO UENUX

Investigadores: Felipe de lima e Lima

Objetivo: Garantir que todos os sistemas da Urna (MSD, Bios, Bootloader, UENUX, APPs e Dados) funcionam de acordo com as especificações de segurança e sejam resistentes a cenários adversos por acaso ou influência de agentes externos. Também é necessário garantir que nenhum dos processos que geram a carga da Urna sejam passiveis de recuperação de dados importantes no término da compilação

Etapas Propostas:

- Verificar a integridade do processo de criação do UENUX:
  - 1. **Processo de build seguro** – Verificar se no computador ou servidor onde o UENUX e seus arquivos foram compilados, o processo de build é seguro de forma que um agente malicioso não seja capaz de recuperar informações importantes da carga da urna como os certificados ou chaves.
- Verificar a integridade e resistência do processo de carga da Urna:
  - 1. **Módulo de mídia inválido ou corrompido** – Gerar uma carga da Urna válida e no meio do processo de carga, arrancar o dispositivo e carregar na urna.
- Verificar a integridade e resistência dos sistemas de segurança:
  - 1. **Segurança da Urna Certificado inválido/ausente da BIOS** – Carregar a urna com certificado inválido/ausente da BIOS e verificar se o MSD bloqueia a urna pela falha criptográfica.
  - 2. **Segurança da Urna Certificado inválido/ausente do Bootloader** – Carregar a urna com certificado inválido/ausente do bootloader e verificar se a BIOS bloqueia a urna pela falha criptográfica.
  - 3. **Segurança da Urna Certificado inválido/ausente do UENUX** – Carregar a urna com certificado inválido/ausente do UENUX e verificar se o Bootloader bloqueia a urna pela falha criptográfica.
  - 4. **Segurança da Urna Certificado inválido/ausente do MSD** – Carregar a urna com certificado inválido/ausente do MSD e verificar se o UENUX bloqueia a urna pela falha criptográfica.
- Verificar a integridade e resistência das urnas em cenários inesperados:

- 1. **Pane de falta de energia na inicialização**– Verificar que o hardware da Urna está preparado para uma pane causada por falta de energia no momento de o eleitor realizar o seu voto na urna. do boot.
- 2. **Pane de falta de energia na execução do Vota** – Verificar que o hardware da Urna está preparado para uma pane causada por falta de energia no momento de o leitor realizar o seu voto na urna.

Resultado: Não executado.

Barreiras derrubadas: Foi disponibilizado amplo acesso às mídias da urna, assim como o seu hardware, sem qualquer limitação de procedimentos ou de lacres físicos.

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de modificar o software da urna, tampouco os seus dados.

PLANO DE TESTE 20: VIOLAR O SIGILO DO VOTO

Investigadores: Ian Martinez Zimmermann e Carlos Alberto da Silva

Objetivo: O teste em questão consiste em acoplar algum tipo de dispositivo, o qual possibilite capturar o áudio disponibilizado para os deficientes visuais e armazenar em alguma mídia para posterior recuperação e identificação da sequência da votação de uma urna eletrônica. Paralelamente, obtém-se a ordem dos eleitores que votaram na respectiva seção eleitoral. Com estas informações em mãos, pretende-se quebrar o sigilo do voto de cada eleitor.

Etapas Propostas:

1. Atacante acessa a urna eletrônica
2. Atacante insere um extensor P2 na saída de áudio da urna
3. Acopla-se o final do extensor P2 ao duplicador de áudio
4. Conecta-se em uma das saídas do duplicador um gravador MP3 habilitado
5. Para cada eleitor, simulando-se mesário, habilita-se o modo acessibilidade
6. inserindo a senha 8888888
7. Dispositivo é retirado da urna
8. Áudios gravados são armazenados e se extraem os votos

Resultado: Plano de teste executado com achado:

Por meio do plug P2 da UE, foi possível quebrar o sigilo do voto, habilitando a saída de áudio para todos os eleitores.

Os votos foram enviados por um transmissor sem fio para um gravador fora do ambiente do TPS.

Soluções sugeridas:

1. Conector proprietário para saída de áudio
2. Aglutinar eleitores que necessitam de áudio em uma seção
3. Treinamento direcionado aos mesários
4. Informar melhor o eleitor
5. UE identifica uso do plug de áudio, como em celulares
6. Adaptador de segurança entre a UE e o fone do eleitor
7. Uso de lacres sobre a saída de áudio

Barreiras derrubadas: O posicionamento da interface de fone de ouvido foi um dificultador para o ataque, pois pressupõe a participação em conluio com o mesário. Mesmo assim, fiscais podem detectar à distância algo conectado no fone de ouvido. Podem ser estudadas novas abordagens via software para logar outros eventos ou mesmo avisar o mesário se há fone de ouvido conectado sem que haja áudio habilitado.

Considerações técnicas: Transmissão do voto à distância via interface de fone de ouvido. Os investigadores utilizaram da saída do fone de ouvido da urna, que fica na face traseira da urna e, portanto, à vista dos fiscais e mesários para conectar um cabo de áudio P2. Esse cabo era conectado depois a um divisor que permitia a conexão de um transmissor Bluetooth ao mesmo tempo em que permitia um extensor de áudio fosse utilizado para a conexão de um fone de ouvido. A ideia era deixar ainda o eleitor com acesso ao fone de ouvido sem que o dispositivo fosse facilmente percebido. O principal obstáculo do ataque é o fato de que o mesário deveria habilitar vários eleitores com áudio para que houvesse uma quantidade substancial que valesse à pena o eventual risco do dispositivo ser percebido, tendo em vista que o áudio não permanece ativado para todos os eleitores, sendo disponibilizado somente para aqueles que precisam desse recurso. Nesse cenário, os eventos de habilitação de vários eleitores com áudio serão registrados no log, fato que poderia ensejar alguma investigação. Destaca-se, ainda, dois pontos: ataque semelhante já foi feito em outra edição do TPS e que o conector e o fio ficam à mostra na face traseira da urna. Ressalta-se, por fim, que hoje já é

apresentada mensagem na tela da urna informando para o eleitor que o áudio está ativado, o que permite ao eleitor verificar se há algo estranho caso não tenha solicitado a ativação desse recurso.

PLANO DE TESTE 22: CAPTURA, ANÁLISE E DECODIFICAÇÃO DE SINAIS ELÉTRICOS COLATERAIS NAS PORTAS EXTERNAS

Investigadores: Nayara Sávia Ayres Alencar (Executado em conjunto com os investigadores Anderson Cunha, Lúcio de Santos Sá e Lucas Pavão de Carvalho Xavier)

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de capturar, armazenar e decodificar possíveis vazamentos de ruídos elétricos decodificáveis de diferentes barramentos que não tenham sido contidos por filtros passivos existentes nas portas.

Etapas Propostas:

1. Medição de sinais elétricos das portas externas por meio de instrumentos durante a digitação por parte do eleitor
2. Uso de dispositivos para captura, amplificação e filtragem desses sinais
3. Uso de software para análise e processamento digital

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi facilitado o ataque com a não utilização de lacres físicos, abertura da urna e fornecimento de documentação de hardware e esquemas elétricos. Não obtiveram sucesso pelo acionamento do timeout do Hardware de Segurança da placa-mãe, pios a urna desligou ao não detectar um sistema operacional autêntico. No caso dos sinais capturados, a criptografia de canal impediu que o sinal fosse decodificado.

Considerações técnicas: Os investigadores conseguiram captar um sinal nas portas USB traseiras semelhantes ao sinal encontrado na interface USB do Teclado do Terminal do Eleitor. Há a hipótese de que o sinal possa ser replicado ou decodificado, mas os investigadores não conseguiram êxito. Outras tentativas foram feitas em trocar o sistema operacional a ser

PLANO DE TESTE 23: ANÁLISE DE DECODIFICAÇÃO DE SINAIS ELETROMAGNÉTICOS À DISTÂNCIA

Investigadores: Lucas Pavão de Carvalho Xavier

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de capturar, armazenar e decodificar sinais eletromagnéticos emitidos pelos circuitos e partes da UE, analisaremos possibilidades de decodificação de informações de dados que violem o sigilo do voto. Empregaremos para as análises equipamentos de laboratório como analisador de espectro, osciloscópio digital, interfaces de captura, circuitos amplificadores e sensores de minha elaboração, componentes eletrônicos para ajustes e softwares de meu desenvolvimento.

Etapas Propostas: Medição de sinais buscando por meio de instrumentos comportamentos eletromagnéticos que ocorram durante as digitações por parte do eleitor. Uso de dispositivos de minha elaboração para captura, amplificação e filtragem. Uso de softwares de minha elaboração para análise e processamento digital.

Resultado: Não executado.

Barreiras derrubadas: Não executado.

Considerações técnicas: O analisador de espectro necessário para o teste não estava funcionando, o que prejudicou sua execução. Mesmo sem a execução, acredita-se que os sinais eletromagnéticos emitidos não possam ser decodificados à distância a ponto de se obter informações, principalmente em um ambiente de seção eleitoral onde o espectro eletromagnético é variado e poluído.

PLANO DE TESTE 24: CAPTURA, ANÁLISE E DECODIFICAÇÃO DE SINAIS ELÉTRICOS COLATERAIS NAS PORTAS EXTERNAS

Investigadores: Lucas Pavão de Carvalho Xavier (Executado em conjunto com os investigadores Anderson Cunha, Lúcio de Santos Sá e Nayara Sávia Ayres Alencar)

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de capturar, armazenar e decodificar possíveis vazamentos de ruídos elétricos decodificáveis de diferentes barramentos que não tenham sido contidos por filtros passivos existentes nas portas.

Etapas Propostas:

1. Medição de sinais elétricos das portas externas por meio de instrumentos durante a digitação por parte do eleitor

2. Uso de dispositivos para captura, amplificação e filtragem desses sinais
3. Uso de software para análise e processamento digital

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi facilitado o ataque com a não utilização de lacres físicos, abertura da urna e fornecimento de documentação de hardware e esquemas elétricos. Não obtiveram sucesso pelo acionamento do timeout do Hardware de Segurança da placa-mãe, pios a urna desligou ao não detectar um sistema operacional autêntico. No caso dos sinais capturados, a criptografia de canal impediu que o sinal fosse decodificado.

Considerações técnicas: Os investigadores conseguiram captar um sinal nas portas USB traseiras semelhantes ao sinal encontrado na interface USB do Teclado do Terminal do Eleitor. Há a hipótese de que o sinal possa ser replicado ou decodificado, mas os investigadores não conseguiram êxito. Outras tentativas foram feitas em trocar o sistema operacional a ser executado.

PLANO DE TESTE 26: INDUÇÃO ELETROMAGNÉTICA

Investigadores: Lucas Pavão de Carvalho Xavier

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de geração de sinais eletromagnéticos, realizar diversos testes com finalidade de afetar o correto registro da vontade do eleitor.

Etapas Propostas: Após análise de sinais e frequências comuns, faremos emissões de sinais acima de qualquer emissão típica normalizada com o objetivo de afetar o funcionamento do teclado e demais dispositivos e funções da UE.

Resultado: Não executado.

Barreiras derrubadas: Não executado.

Considerações técnicas: Não executado.

PLANO DE TESTE 27: INSERÇÃO DE SERVIÇO NÃO AUTORIZADO NO SIS

Investigadores: Lucas Pavão de Carvalho Xavier

Objetivo: Inserir serviço e iniciar com sucesso dentro de Windows preparado com o SIS. As políticas de segurança do SIS são baseadas em API do Windows, mas não é claro o alcance dos controles.

Etapas Propostas: Inicialização de máquina usando sistema operacional paralelo, inserção de arquivos, escrita de scripts de inserção de chaves no registro do Windows.

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Fornecimento de credencial para autenticação no SIS.

Considerações técnicas: Não houve sucesso em virtualizar o SIS, pois o disco se encontra cifrado com bitlocker com senha no TPM.

PLANO DE TESTE 29: ALTERAÇÃO DO TEOR DOS ARQUIVOS NA MÍDIA DE PREPARAÇÃO – PÓS GEDAI-UE

Investigadores: Lucas Pavão de Carvalho Xavier

Objetivo: Alteração da mídia de preparação com alvo final na alteração de imagens dos candidatos. Os softwares fundamentais e diversas imagens têm hashs registrados e confirmados, procedimento que possivelmente não atinge imagens dos candidatos.

Etapas Propostas: Análise das estruturas dos arquivos, decodificação, alteração e gravação de novos arquivos.

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado amplo acesso às mídias da urna, assim como o seu hardware, sem qualquer limitação de procedimentos ou de lacres físicos.

Considerações técnicas: Nenhum achado. Os investigadores não foram capazes de alterar arquivos nas mídias da urna.

PLANO DE TESTE 30: SISTEMA/PROGRAMA TRANSPORTADOR DE ARQUIVOS (JE CONNECT)

Investigadores: Rodrigo Cardoso Silva

Objetivo: Analisar o processo de envio das Mídia de Registro dos Votos (MRV) mediante ao servidor receptor TSE

Etapas Propostas:

1. Verificar o tipo de VPN para descobrir se baseiam algoritmos de hash MD5 ou SHA-1 e protocolos PPTP ou L2TP/IPSec

2. Descobrir as chaves mestres da VPN

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Fornecimento do PIN;

Considerações técnicas: Não conseguiu superar a barreira do JE Connect que impede sua execução em máquina virtual;

PLANO DE TESTE 31: VITRUVIANO

Investigadores: Kennedy Antônio Vasconcelos Ferreira Júnior

Objetivo: O teste será realizado na simulação da gravação dos dados registrados nas urnas pelo ASN.1 na encapsulação do código-fonte e as assinaturas, e posteriormente gravando um código de funcionamento falso, utilizando o RDV para força a validação de informações gravadas no RED de forma incorreta.

Etapas Propostas:

1. Registro das informações e comandos na assinatura ASN.1
2. Tentativa de acessar a URL HTTPS
3. Validar uma informação não verdadeira carregada no sistema RecArquivos

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi disponibilizado amplo acesso às mídias da urna, assim como o seu hardware, sem qualquer limitação de procedimentos ou de lacres físicos. Nenhum procedimento de controle relativo à contingência de urna ou recuperação de resultados foi aplicado, sendo possível a livre execução do software da urna.

Considerações técnicas: Nenhum achado. O investigador não foi capaz de alterar arquivos nas mídias da urna.

PLANO DE TESTE 32: CAPTURA, ANÁLISE E DECODIFICAÇÃO DE SINAIS ELÉTRICOS COLATERAIS NAS PORTAS EXTERNAS

Investigadores: Lucas Pavão de Carvalho Xavier (Executado em conjunto com os investigadores Anderson Cunha, Lúcio de Santos Sá e Nayara Sávia Ayres Alencar)

Objetivo: Por meio de dispositivos desenvolvidos e ajustados com a finalidade de capturar, armazenar e decodificar possíveis vazamentos de ruídos elétricos decodificáveis de diferentes barramentos que não tenham sido contidos por filtros passivos existentes nas portas.

Etapas Propostas:

1. Medição de sinais elétricos das portas externas por meio de instrumentos durante a digitação por parte do eleitor
2. Uso de dispositivos para captura, amplificação e filtragem desses sinais
3. Uso de software para análise e processamento digital

Resultado: Plano de teste executado sem achados.

Barreiras derrubadas: Foi facilitado o ataque com a não utilização de lacres físicos, abertura da urna e fornecimento de documentação de hardware e esquemas elétricos. Não obtiveram sucesso pelo acionamento do timeout do Hardware de Segurança da placa-mãe, pios a urna desligou ao não detectar um sistema operacional autêntico. No caso dos sinais capturados, a criptografia de canal impediu que o sinal fosse decodificado.

Considerações técnicas: Os investigadores conseguiram captar um sinal nas portas USB traseiras semelhantes ao sinal encontrado na interface USB do Teclado do Terminal do Eleitor. Há a hipótese de que o sinal possa ser replicado ou decodificado, mas os investigadores não conseguiram êxito. Outras tentativas foram feitas em trocar o sistema operacional a ser executado.

SOLUÇÕES E TESTE DE CONFIRMAÇÃO

As respectivas soluções estão sendo analisadas e as implementações serão conduzidas de acordo com os processos utilizados no desenvolvimento dos sistemas eleitorais da STI/TSE.

Para que as soluções sejam validadas, será realizado, no período de 11 a 13/05/2022, um novo teste, denominado Teste de Confirmação, conforme prevê o Edital do TPS:

> *Art. 37. Em data estabelecida no Marco 20 do Calendário do Evento, os investigadores e/ou grupos de investigadores serão convocados, pelo TSE, a repetirem, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.*
>
> *§ 1º Na hipótese prevista no caput, os investigadores e/ou grupo de investigadores serão notificados para comparecer ao teste de confirmação, via carta registrada ou e-mail com aviso de recebimento, devendo ser justificada possível ausência.*
>
> *§ 2º Durante o Teste de Confirmação, será disponibilizada visualização do código-fonte no ambiente de apresentação, conforme o art. 33 deste edital.*
>
> *§ 3º A nova execução dos testes 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.*
>
> *§ 4º As modificações realizadas serão apresentadas no período de realização do Teste de Confirmação, conforme o Marco 20, estabelecido no Calendário de Eventos.*
>
> *§ 5º Os grupos de investigadores poderão ser representados por apenas um de seus componentes, exceto se houver, no grupo, mais de um componente que recebeu diárias e passagens custeadas pela Justiça Eleitoral cuja presença é obrigatória, sob pena de devolução dos valores.*
>
> *§ 6º Uma vez realizados os novos testes e tendo sido comprovado o saneamento das vulnerabilidades anteriormente encontradas, os investigadores e/ou grupo de investigadores deverão assinar termo com a confirmação das correções feitas.*