Relatório final da Comissão Avaliadora

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 588 de 10 de setembro de 2021, 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 é composta por 11 membros, representantes dos seguintes órgãos:

- TSE – Dr. Sandro Nunes Vieira
- MPF – Patricia Sumie Hayakawa
- Congresso Nacional – Robson Paniago de Miranda
- OAB – Rodrigo Lemgruber
- PF – Perito Criminal Thiago de Sá Cavalcanti
- TCU – Auditor André Luiz Furtado Pacheco
- CONFEA – Rodrigo de Souza Borges
- SBC – Professor Doutor Rafael Timóteo de Sousa Júnior
- Comunidade Acadêmica – Professor Doutor Mamede Lima-Marques
- Comunidade Acadêmica – Doutor Osvaldo Catsumi Imamura
- Comunidade Acadêmica – Professor Doutor Jamil Salem Barbar

O propósito deste relatório é apresentar os resultados dos testes dos investigadores e grupos de investigadores.

2 Metodologia de Avaliação dos Testes

Foram mantidos os critérios de análise do TPS 2019, ou seja:

- Pontos de intervenção: elementos do processo eleitoral atacados;
- Impacto: quais propriedades de segurança foram violadas;
- Extensão: granularidade, extensão geográfica (ex. urna, seção etc.);
- Contexto: procedimentos, atores, circunstâncias do processo eleitoral.

Foi mantida a classificação dos resultados dos Planos de Teste como:

- Não realizados;

- Realizados sem contribuição para melhoria do sistema;
- Realizados com contribuição para melhoria do sistema.

3 Planos de Teste Aprovados

Foram recebidos 32 planos de teste e a Comissão Reguladora aprovou 29 planos e 3 foram rejeitados. Os objetos das propostas foram os seguintes:

1. **Plano de Teste 01 (*Invasão ao JEConnect*):**
   - Coordenador: Fellipe Ribeiro Silva Abib
   - Componentes do Grupo: Caio Henrique de Aquino Vicente, Charles William Biesseki, Alan Papafanurakis Heleno
   - Resumo do teste: Acessar o JEConnect para extrair a conexão VPN com o TSE e assim possuir um acesso direto para explorar os softwares diretamente.

2. **Plano de Teste 02 (*Rastrear a ordem da votação dentro do BU*):**
   - Coordenador: Thiago Silva Mazzante
   - Componentes do Grupo: Felipe Fonteles Belo
   - Resumo do teste: Rastrear e identificar a ordem da votação dentro de uma urna eletrônica.

3. **Plano de Teste 03 (*Verificação do comportamento do parâmetro urna:* `mcriptografar`):**
   - Investigador individual: André Luiz de Matos
   - Resumo do teste: Foi verificado durante a abertura de investigação do código fonte um conjunto de parametrizações da urna que compõem a compilação do código para carga inicial. Dentre estes parâmetros, identificou-se o parâmetro `mcriptografar` - com parametrização default (*True*). Entendemos ser uma possível vulnerabilidade porque poderia desabilitar a criptografia com sua alteração. Precisamos avaliar o comportamento resultante com o parâmetro modificado.

4. **Plano de Teste 04 (*Invasão leiga: Soldadinho-do-Araripe*):**
   - Investigador individual: Gabriel Leonardo de Sena Santos
   - Resumo do teste: Propõe-se testar uma alteração no SCUE, que simularia uma instabilidade no sistema. Sendo necessário a substituição da urna e recuperação da dos dados já armazenados. Assim, seria necessário colher os dados armazenados no RED.

5. **Plano de Teste 05 (*Modificação do BU e RDV (total de votos), para teste de validação de assinatura*):**
   - Coordenador: IMED – Faculdade Meridional
   - Componentes do Grupo: Marcos Roberto dos Santos; Adroaldo Leão Souto Júnior; Juliano Ribeiro Poli; Gabriel Sordi Damo; Vinícius Borges Fortes

- Resumo do teste: Alteração do arquivo que contém os votos gerados pela urna e teste de envio com nova assinatura gerada com chave fake.

6. **Plano de Teste 06 (*Teste não intrusivo da urna eletrônica 2015 (keylogger não intrusivo)*):**
   - Coordenador: IMED – Faculdade Meridional
   - Componentes do Grupo: Marcos Roberto dos Santos; Adroaldo Leão Souto Júnior; Juliano Ribeiro Poli; Gabriel Sordi Damo; Vinícius Borges Fortes
   - Resumo do teste: Será colocado um invólucro na urna com o objetivo de coletar os votos, relacionando os mesmos com o *timestamp*.

7. **Plano de Teste 07 (*Recuperação de dados sensíveis enviados via método GET*):**
   - Investigador individual: Lucio Santos de Sá
   - Resumo do teste: 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.

8. **Plano de Teste 08 (*Executar JE Connect em máquina com firmware de componente não proprietário e não assinado*):**
   - Investigador individual: Lucio Santos de Sá
   - Resumo do teste: Instalar firmware próprio em componente da máquina que receberá o JE Connect, sem que este esteja assinado digitalmente para testar a possibilidade de execução de RootKit em ambiente seguro.

9. **Plano de Teste 09 (*Identificar teclas pressionadas através do retorno tátil sonoro do teclado da Urna Eletrônica*):**
   - Investigador individual: Lucio Santos de Sá
   - Resumo do teste: 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.

10. **Plano de Teste 10 (*Execução de ataques de agente autorizado com o uso do JE Connect*):**
    - Investigador individual: Lucio Santos de Sá
    - Resumo do teste: Após a análise de código, foi observado que alguns dos sistemas de uso autenticado do JE Connect possuíam a proteção contra Cross *Site S*cripting 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*.

11. **Plano de Teste 11 (*Alteração de informações da tabela de correspondência*):**

- Coordenador: Paulo César Herrmann Wanner
- Componentes do Grupo: Ivo de Carvalho Peixinho, Galileo Batista de Sousa
- Resumo do teste: 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.

12. Plano de Teste 12 (*Extração de dados e configurações do Kit JE Connect*):
- Coordenador: Paulo César Herrmann Wanner
- Componentes do Grupo: Ivo de Carvalho Peixinho, Galileo Batista de Sousa
- Resumo do teste: 1. Obter senhas e configuração da VPN a partir de uma mídia do JE Connect. 2. A partir dos dados obtidos tentar se conectar diretamente à rede do TSE. 3. Verificar a existência de vulnerabilidades no RecArquivos utilizando técnicas de *fuzzing* 4. Verificar a possibilidade de acesso direto ao banco de dados e as suas rotinas.

13. Plano de Teste 13 (*Captura, análise e decodificação de sinais elétricos colaterais nas portas externas*):
- Investigador individual: Anderson Cunha da Costa
- Resumo do teste: Captura, análise e decodificação de sinais elétricos nas portas expostas.

14. Plano de Teste 14 (*Registro digital do voto e ordem de votação: possível quebra de sigilo*):
- Investigador individual: Lorenna Rodrigues Tredezini
- Resumo do teste: Possibilidade de quebra do sigilo do voto quando da gravação dos dados a ele relativos para o Registro Digital do Voto.

15. Plano de Teste 15 (*GUEDAI-UE, SAVP-Sortei e Votacao e Módulo*):
- Investigador individual: Felipe de Lima e Lima
- Resumo do teste: Garantir a integridade e segurança do GUEDAI-EU e outros sistemas da empresa Módulo e outros sub-sistemas de segurança.

16. Plano de Teste 16 (*Segurança do JE Connect e do Firefox*):
- Investigador individual: Felipe de Lima e Lima
- Resumo do teste: Garantir a integridade e segurança do JE Connect com o Firefox em cenários de falha e cenários de ataque diversos, pois esses são executados em ambientes fora do controle do TSE.

17. Plano de Teste 17 (*Segurança do REC-Arquivos e Info-Arquivos*):
- Investigador individual: Felipe de Lima e Lima

- Resumo do teste: Garantir a integridade e segurança do Info-Arquivos e Rec-Arquivos nas suas execuções.

18. Plano de Teste 18 (*Sistot, Transportador e Transportador Backend*):
- Investigador individual: Felipe de Lima e Lima
- Resumo do teste: Garantir a integridade e segurança do Transportador e Transportador Backend pois este pode vazar informações sensíveis sobre os votos no momento de transmissão entre os pontos de contato com o TSE.

19. Plano de Teste 19 (*MSD, Bios, Bootloader, UENUX, APPs e Dados & Processo de compilação do UENUX*):
- Investigador individual: Felipe de Lima e Lima
- Resumo do teste: Garantir a integridade e segurança do UENUX para cenários de ataque e falhas externas, assim como possíveis vazamentos de informações que podem ocorrer no processo de geração da carga e compilação.

20. Plano de Teste 20 (*Violar o sigilo do voto*):
- Coordenador: Carlos Alberto da Silva
- Componentes do Grupo: Ian Martinez Zimmermann
- Resumo do teste: O TSE garante o direito do voto a todos os cidadãos, incluindo aquelas pessoas com deficiência visual. Neste contexto, as urnas eletrônicas proporcionam a inclusão social desses cidadãos. Basicamente, consiste de uma fonte de ouvido no qual o deficiente visual, ao digitar nas teclas identificada por impressão em braile, pode-se ouvir o número digitado, ratificando sua opção de voto. A tentativa de violar o sigilo do voto, consiste em capturar o áudio disponibilizado por esta saída de áudio, e consequentemente, a quebrar o sigilo do voto para pessoas com ou sem deficiência visual durante o processo de votação, observando a ordem dos votantes da respectiva seção eleitoral.

21. Plano de Teste 21 [REPROVADO] (*Transparência e adequação da política de proteção de dados pessoais à Luz da Lei Geral de Proteção de Dados – LGPD no sistema eletrônico de Votação a partir de experimentos no teste público de segurança- TPS*):
- Coordenador: Tatiana dos Santos Gomes Franca
- Componentes do Grupo: Mariana Lagares de Paula, Josy Martins da Ressurreição, Maria Helena Lopes Sales, Thayser Stanys Coelho Berwian Schneider
- Resumo do teste: Inicialmente destacamos que nossa participação no TPS 2021 ocorreu de forma interdisciplinar onde buscamos compreender o sistema eletrônico e observar a segurança jurídica do processo, enquanto operadores do direito e levar à sociedade por meio da comunicação jornalística uma espécie de tradução do evento. Nossa proposta se dá a partir da observação realizada na etapa da abertura do código-fonte, por meio de dedução lógica para argumentar

acerca das possibilidades de falhas durante os processos de preparação da urna, votação e apuração no que se refere aos dados pessoais inseridos no processo.

22. **Plano de Teste 22 (*Captura, análise e decodificação de sinais elétricos colaterais nas portas externas*):**
    - Investigador individual: Nayara Sávia Ayres Alencar
    - Resumo do teste: Captura, análise e decodificação de sinais elétricos nas portas expostas.

23. **Plano de Teste 23 (*Análise e decodificação de sinais eletromagnéticos a distância*):**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Análise e decodificação de sinais eletromagnéticos a distância.

24. **Plano de Teste 24 (*Captura, análise e decodificação de sinais elétricos colaterais nas portas externas*:**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Captura, análise e decodificação de sinais elétricos nas portas expostas.

25. **Plano de Teste 25 [REPROVADO] (*Desvio de destinos e rotas TCP/IP e criação de ambiente falso de recepção TSE*):**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Desvio de destinos DNS e gateways e criação de ambiente simulado de recepção de arquivos;

26. **Plano de Teste 26 (*Indução eletromagnética*):**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Indução de sinais eletromagnéticos com finalidade de acionar teclas, atrapalhar o registro ou modificar a vontade do eleitor.

27. **Plano de Teste 27 (*Inserção de serviço Windows não autorizado no SIS*):**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Criação de chave de serviço, inserção de executável e inicialização dentro do ambiente SIS.

28. **Plano de Teste 28 [REPROVADO] (*Substituição dos navegadores web por versões adulteradas*):**
    - Investigador individual: Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Substituição dos executáveis de navegadores web usados por versões adulteradas.

29. **Plano de Teste 29 (*Alteração do teor dos arquivos na mídia de preparação – pós GEDAI-UE*):**

- Investigador individual: Lucas Pavão de Carvalho Xavier
- Resumo do teste: Alteração da mídia de preparação inserindo arquivos manipulados com sucesso na UE.

30. **Plano de Teste 30 (*Sistema/Programa Transportador de Arquivos (JE-Connect)*):**
    - Investigador individual: Rodrigo Cardoso Silva
    - Resumo do teste: Analisar o processo de envio das Mídia de Registro dos Votos (MRV) mediante ao servidor receptor TSE para: a) Verificar o tipo de VPN para descobrir se baseiam algoritmos de *hash* MD5 ou SHA-1 e protocolos PPTP ou L2TP/IPSec; e b) Descobrir as chaves mestres da VPN.

31. **Plano de Teste 31 (*Vitruviano*):**
    - Investigador individual: Kennedy Antônio Vasconcelos Ferreira Júnior
    - Resumo do teste: Teste a ser realizado na simulação da gravação dos dados registrados nas urnas pelo ASN.1 na encapsulação do código-fonte e as assinaturas, e posteriormente fraudado, utilizando o RDV com informações gravadas no RED.

32. **Plano de Teste 32 (*Captura, análise e decodificação de sinais elétricos colaterais nas portas externas*):**
    - Investigador individual: Lúcio Santos de Sá
    - Resumo do teste: Captura, análise e decodificação de sinais elétricos nas portas expostas.

4 Planos de Teste Executados

Os investigadores presentes no TPS identificaram alguns testes com propostas similares, ou complementares, e decidiram unir os esforços formando inicialmente 15 grupos de investigação e finalizando os testes em 13 grupos, coordenados pela Comissão Reguladora.

Desta forma, para tornar os trabalhos de avaliação consistentes com o andamento das investigações e com os registros efetuados pela Equipe de Apoio Técnico do TPS 2021, constituída para acompanhar as atividades, registra-se a seguir os planos efetivamente executados pelos grupos formados durante os testes.

1. **Grupo 1: Invasão Leiga – Soldadinho do Araripe**
    - Investigador(es): Gabriel Leonardo de Sena Santos
    - Resumo do teste: Propõe-se testar uma alteração no SCUE, que simularia uma instabilidade no sistema. Sendo necessário a substituição da urna e recuperação da dos dados já armazenados. Assim, seria necessário colher os dados armazenados no RED.
    - Plano de Teste Proposto: 4

2. **Grupo 2: Verificação do comportamento do parâmetro urna: `mcriptografar`**
   - Investigador(es): André Luiz de Matos
   - Resumo do teste: Foi verificado durante a abertura de investigação do código fonte um conjunto de parametrizações da urna que compõem a compilação do código para carga inicial. Dentre estes parâmetros, identificou-se o parâmetro `mcriptografar` - com parametrização default (*True*). Entendemos ser uma possível vulnerabilidade porque poderia desabilitar a criptografia com sua alteração. Precisamos avaliar o comportamento resultante com o parâmetro modificado.
   - Plano de Teste Proposto: 3

3. **Grupo 3: Invasão ao JEConnect**
   - Investigador(es): Fellipe Ribeiro Silva Abib, Caio Henrique de Aquino Vicente, Charles William Biesseki, Alan Papafanurakis Heleno
   - Resumo do teste: Acessar o JEConnect para extrair a conexão VPN com o TSE e assim possuir um acesso direto para explorar os softwares diretamente.
   - Plano de Teste Proposto: 1

4. **Grupo 4: Rastrear a ordem de votação dentro do BU**
   - Investigador(es): Thiago Silva Mazzante, Felipe Fonteles Belo
   - Resumo do teste: Rastrear e identificar a ordem da votação dentro de uma urna eletrônica.
   - Plano de Teste Proposto: 2

5. **Grupo 5: Captura, análise e decodificação de sinais elétricos colaterais nas portas externas**
   - Investigador(es): Anderson Cunha da Costa
   - Resumo do teste: Captura, análise e decodificação de sinais elétricos nas portas expostas.
   - Plano de Teste Proposto: 13 (trabalhou com os Grupos 8, 14 e 15)

6. **Grupo 6: Sistema/Programa Transportador de Arquivos (JE-Connect)**
   - Investigador(es): Rodrigo Cardoso Silva
   - Resumo do teste: Analisar o processo de envio das Mídia de Registro dos Votos (MRV) mediante ao servidor receptor TSE para: a) Verificar o tipo de VPN para descobrir se baseiam algoritmos de *hash* MD5 ou SHA-1 e protocolos PPTP ou L2TP/IPSec; e b) Descobrir as chaves mestres da VPN.
   - Plano de Teste Proposto: 30 (trabalhou junto com o Grupo 14)

7. **Grupo 7: Vitruviano**
   - Investigador(es): Kennedy Antônio Vasconcelos Ferreira Júnior
   - Resumo do teste: Teste a ser realizado na simulação da gravação dos dados registrados nas urnas pelo ASN.1 na encapsulação do código-fonte e as assinaturas, e posteriormente fraudado, utilizando o RDV com informações gravadas no RED.
   - Plano de Teste Proposto: 31

8. **Grupo 8: Captura, análise e decodificação de sinais elétricos nas portas externas**
   - Investigador(es): Nayara Sávia Ayres Alencar
   - Resumo do teste:Captura, análise e decodificação de sinais elétricos nas portas expostas.
   - Plano de Teste Proposto: 22 (trabalhou com os Grupos 5, 14 e 15)

9. **Grupo 9: Registro Digital do Voto e Ordem de Votação: Possível Quebra de Sigilo**
   - Investigador(es): Lorenna Rodrigues Tredezzini
   - Resumo do teste: Possibilidade de quebra do sigilo do voto quando da gravação dos dados relativos a ele para o Registro Digital do Voto.
   - Plano de Teste Proposto: 14

10. **Grupo 10: Violar o sigilo do voto**
    - Investigador(es): Carlos Alberto da Silva, Ian Martinez Zimmermann
    - Resumo do teste: O TSE garante o direito do voto a todos os cidadãos, incluindo aquelas pessoas com deficiência visual. Neste contexto, as urnas eletrônicas proporcionam a inclusão social desses cidadãos. Basicamente, consiste de uma fonte de ouvido no qual o deficiente visual, ao digitar nas teclas identificada por impressão em braile, pode-se ouvir o número digitado, ratificando sua opção de voto. A tentativa de violar o sigilo do voto, consiste em capturar o áudio disponibilizado por esta saída de áudio, e consequentemente, a quebrar o sigilo do voto para pessoas com ou sem deficiência visual durante o processo de votação, observando a ordem dos votantes da respectiva seção eleitoral.
    - Plano de Teste Proposto: 20

11. **Grupo 11: Modificação dos dados do BU e RDV (total de votos), para teste de validação de assinatura; e Teste não intrusivo da UE2015 (Keylogger não intrusivo).**

- Investigador(es): Marcos Roberto dos Santos; Adroaldo Leão Souto Júnior; Juliano Ribeiro Poli; Gabriel Sordi Damo
- Resumo do teste: Alteração do arquivo que contém os votos gerados pela urna e teste de envio com nova assinatura gerada com chave fake. Será colocado um invólucro na urna com o objetivo de coletar os votos, relacionando os mesmos com o *timestamp*.
- Plano de Teste Proposto: 5 e 6

12. **Grupo 12: Alteração de informações da tabela de correspondência; e Extração de dados e Configuração do Kit JE Connect**
    - Investigador(es): Paulo César Herrmann Wanner, Ivo de Carvalho Peixinho, Galileo Batista de Sousa
    - Resumo do teste: 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.6) Obter senhas e configuração da VPN a partir de uma mídia do JE Connect. 7) A partir dos dados obtidos tentar se conectar diretamente à rede do TSE. 8) Verificar existência de vulnerabilidades no RecArquivos utilizando técnicas de *fuzzing*. 9) Verificar a possibilidade de acesso direto ao banco de dados e as suas rotinas.
    - Plano de Teste Proposto: 11 e 12

13. **Grupo 13: Segurança do JE Connect e do Firefox; Segurança do REC-Arquivos e Info-Arquivos; Sistot, Transportador e Transportador Backend; MSD, Bios, Bootloader, UENUX, APPs e Dados & Processo de compilação do UENUX**
    - Investigador(es): Felipe de Lima e Lima
    - Resumo do teste: Garantir a integridade e segurança do JE Connect com o Firefox em cenários de falha e cenários de ataque diversos, pois esses são executados em ambientes fora do controle do TSE. Garantir a integridade e segurança do Info-Arquivos e Rec-Arquivos nas suas execuções. Garantir a integridade e segurança do Transportador e Transportador Backend pois este pode vazar informações sensíveis sobre os votos no momento de transmissão entre os pontos de contato com o TSE. Garantir a integridade e segurança do UENUX para cenários de ataque e falhas externas, assim como possíveis vazamentos de informações que podem ocorrer no processo de geração da carga e compilação.
    - Plano de Teste Proposto: 16, 17, 18 e 19

14. **Grupo 14: Recuperação de dados sensíveis enviados via método GET (JEC Connect); Executar J Connect em máquina com firmware de componente não proprietário e não assinado; Identificar teclas pressionadas através do retorno tátil sonoro do teclado da Urna Eletrônica; Execução de ataques de agente autorizado com o uso do JE Connect; Captura, análise e decodificação de sinais elétricos colaterais nas portas externas.**
    - Investigador(es): Lúcio Santos e Sá
    - Resumo do teste: 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. Instalar firmware próprio em componente da máquina que receberá o JE Connect, sem que este esteja assinado digitalmente para testar a possibilidade de execução de RootKit em ambiente seguro. 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. Após a análise de código, foi observado que alguns dos sistemas de uso autenticado do JE Connect possuíam a proteção contra Cross *Site S*cripting 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*. Captura, análise e decodificação de sinais elétricos nas portas expostas.
    - Plano de Teste Proposto: 7, 8, 9, 10 e 29 (trabalhou junto com o Grupo 6, 5, 8 e 15)

15. **Grupo 15: Análise e decodificação de sinais eletromagnéticos a distância. Captura, análise e decodificação de sinais elétricos colaterais nas portas externas, Indução eletromagnética. Inserção de serviço Windows não autorizado no SIS. Alteração do teor dos arquivos na mídia de preparação pós GEDAI-UE.**
    - Investigador(es): Lucas Pavão de Carvalho Xavier
    - Resumo do teste: Análise e decodificação de sinais eletromagnéticos a distância. Captura, análise e decodificação de sinais elétricos nas portas expostas. Indução de sinais eletromagnéticos com finalidade de acionar teclas, atrapalhar o registro ou modificar a vontade do eleitor. Criação de chave de serviço, inserção de executável e inicialização dentro do ambiente SIS. Alteração da mídia de preparação inserindo arquivos manipulados com sucesso na UE.
    - Plano de Teste Proposto: 23, 24, 26, 27 e 29 (trabalhou com os Grupos 5, 8 e 14)

5 Avaliação dos Planos de Teste

Os planos de teste apresentados em consequência ao edital de Testes Públicos de Segurança do Sistema Eletrônico de Votação foram todos avaliados pela Comissão Avaliadora. Os resultados da realização dos planos são apresentados a seguir:

5.1 Planos de teste não realizados

Os planos de testes 18 e 26 não foram realizados.

5.2 Planos de teste realizados sem contribuições

Os planos de teste realizados que não obtiveram sucesso no alcance dos objetivos propostos foram: 1, 2, 5, 7, 8, 9, 10, 11, 13, 14, 15, 17,19, 22, 23, 24, 27, 29, 30, 31 e 32.

5.3 Planos de teste realizados com contribuição

Os planos de teste que apresentaram resultados de avanço nos objetivos propostos foram: 3, 4, 6, 12, 16 e 20.

5.3.1 Plano de teste 3

O investigador percebeu um parâmetro no código fonte (`mcriptografar`) que tinha a sua condição inicial de operação de forma explícita e que isso poderia comprometer a integridade do Boletim de Urna (BU) gerado, caso essa condição fosse alterada.
Não obtendo êxito nas tentativas no arquivo de configuração, foi solicitado à equipe técnica de apoio a alteração dessa condição inicial para não criptografar, deixando-o em claro.
O BU, com as modificações realizadas no seu conteúdo, foi transmitido, mas rejeitado por inconsistência durante a verificação da sua assinatura digital no processo de transmissão.
Todavia, foi percebido que o BU original era recebido e validado mesmo sendo transmitido em claro, somente com a sua assinatura digital.
A equipe técnica da Justiça Eleitoral informa que o procedimento de configuração da criptografia do BU existe no sistema da Urna Eletrônica para permitir a geração de BU em claro quando a mesma for cedida para ser utilizada em eleições na sociedade.

Avaliação

A alteração da configuração para não criptografar o BU não apresentou nenhuma anomalia no comportamento do sistema de transmissão e recepção do BU, pois o sistema verifica somente a assinatura do arquivo. A princípio, o sistema de transmissão e recepção do BU é somente um meio de transporte de arquivo eletrônico de forma segura, verificando se o arquivo recebido é o mesmo transmitido, o que foi comprovado no teste. A abertura do BU é resolvida na instância posterior ao recebimento do BU.
Cabe à Justiça Eleitoral analisar e registrar os riscos associados ao uso da criptografia nas eleições oficiais.

5.3.2 Plano de teste 4

O objetivo do teste foi a verificação do processo de contingência das urnas eletrônicas.
O teste consiste em gerar um falso pedido de contingência de urna e gerar resultados em ambas as urnas e transmiti-los.
O investigador verificou os procedimentos de contingência de urnas eletrônicas gerando todas as possibilidades e a continuidade da votação, uma vez que a falha foi simulada somente por meio de desligamento da urna permitindo o seu retorno ao funcionamento a qualquer momento.

Avaliação

O processo de contingência das urnas durante a realização de uma eleição faz parte do processo de continuidade de forma eficaz, garantindo a integridade das informações constantes na urna original e na de contingência utilizada.
O investigador constatou no teste o funcionamento do processo de contingência, a substituição da urna eletrônica em caso de constatação de uma falha não recuperável, adotado pela Justiça Eleitoral.
Um ataque no processo de contingência, na forma como foi proposto pelo investigador, necessita de participação de vários elementos humanos envolvidos na seção eleitoral, o registro da substituição na ata e também uma série de registros nos arquivos de log da urna, indicando uma situação anormal.
A vulnerabilidade associada à segurança da eleição, neste caso, reside nos procedimentos estabelecidos para a realização da verificação da falha da urna original, a decisão em utilizar uma urna de contingência para dar continuidade à votação pelos eleitores e o registro do ocorrido na ata da seção. As normas e as instruções que orientam o funcionamento de uma seção eleitoral são a garantia da segurança e da integridade do processo.

5.3.3 Plano de teste 6

O teste consiste na instalação de uma capa no teclado da urna eletrônica, devidamente projetada, munida de sensores capazes de transmitir todas as teclas pressionadas pelo eleitor para o registro do seu voto, possibilitando a coleta dos votos à distância.
O dispositivo protótipo foi muito bem construído cobrindo toda superfície frontal da urna, dificultando a percepção da alteração efetuada na urna. O funcionamento ocorreu de forma planejada possibilitando a leitura de todas as teclas utilizadas na urna durante uma votação.

Avaliação

Teste realizado com sucesso, demonstrando que há meios para acompanhar uma votação identificando todas as telas utilizadas pelo eleitor na urna eletrônica.
A viabilidade do emprego da proposta apresentada é uma questão que deve ser acompanhada pela Justiça Eleitoral pois a disponibilidade da engenharia da tecnologia a ser utilizada pode ocorrer a qualquer momento, impactando na atenção necessária dos mesários na seção eleitoral.

5.3.4 Plano de teste 12

A proposta de teste de obtenção dos dados de configuração e senhas gravadas internamente no sistema do kit de transmissão de dados de eleição foram executadas com relativo sucesso. As senhas de acesso aos aplicativos e de inicialização foram fornecidas após algumas tentativas sem sucesso.
A partir desse ponto, os investigadores conseguiram avançar nos seus planos e obter as chaves gravadas internamente no sistema e obtendo o controle de acesso às partições do disco do computador alvo.
Os resultados obtidos demonstraram que um usuário interno habilitado somente para ativar o aplicativo de transmissão de dados pode chegar a partes do sistema que deveriam estar protegidos para impedir acesso a outros recursos do computador e da rede.
Apesar do acesso à VPN (rede com conexão protegida), não obtiveram sucesso para observar os detalhes da porta conectada no destino por conta dos demais mecanismos de segurança de rede existentes.
A configuração do ambiente estava simulando o período eleitoral e a senha de acesso expirou às 20h da sexta-feira, forçando a inicialização de todo o processo no dia seguinte com uma nova senha (“oficial” para as eleições), liberada somente no dia anterior das eleições.

Avaliação

O teste demonstra uma vulnerabilidade de acesso à rede que, mesmo estando protegida por outros mecanismos e contendo a invasão exclusivamente no ambiente definido pelo canal da VPN, pode permitir o desenvolvimento de ações que podem gerar novos riscos de ataques.
A Justiça Eleitoral deve reavaliar os riscos envolvidos em todas as partes que compõem o ambiente de transmissão e recepção de dados da eleição.

5.3.5 Plano de teste 16

O teste objetiva ter acesso à rede por meio do aplicativo de transmissão de dados (JE Connect).
O investigador verificou uma vulnerabilidade existente no acesso à rede do aplicativo copiando o caminho em uma outra seção do navegador, como se fosse uma nova requisição de acesso, e conseguiu navegar na rede com sucesso.

Avaliação

O uso de produtos comerciais deve ser estudado com cuidado pela Justiça Eleitoral por terem sido desenvolvidos para garantir as facilidades necessárias para a navegação na rede de dados.
Como a restrição de acesso à rede foi um requisito estabelecido para a aplicação (JE Connect) e a sua camada externa de proteção (SIS) e não para o navegador web (Firefox), que faz parte integrante do sistema de transmissão, a vulnerabilidade foi bem explorada pelo investigador.
A Justiça Eleitoral deve revisar e reavaliar os requisitos de segurança e o plano de risco para esta ferramenta como um todo.

5.3.6 Plano de teste 20

O investigador testou a possibilidade de utilização da saída de áudio da urna eletrônica para transmitir todo o processo existente de acessibilidade para os eleitores com deficiência visual.
A vulnerabilidade explorada não se limita aos casos de deficientes visuais, uma vez que essa facilidade de áudio pode ser utilizada por um eleitor que tenha dificuldade em ler e interpretar as mensagens apresentadas na tela, ou para confirmar os números digitados, desde que habilitado pelo mesário para cada eleitor.

Avaliação

A opção de utilização de áudio para realizar uma votação é uma facilidade necessária para garantir a inclusão dos eleitores que apresentarem alguma

dificuldade em operar uma urna somente por meio das interfaces visuais e tácteis. Uma das vulnerabilidades da interface auditiva é o seu uso indevido, como foi o caso do teste proposto.
O risco existente está mitigado por meio de procedimentos adotados na seção eleitoral, devendo os mesários e os técnicos de apoio observar a preservação da interface auditiva sob controle durante a realização de uma votação e registrar todos os momentos da sua utilização. O eleitor que não tenha deficiência visual e que venha solicitar a utilização desta facilidade durante a votação poderá constatar a ativação da saída de áudio por meio de um indicador visual presente na tela da urna.
A ata da seção eleitoral deve constar a habilitação e o uso da interface auditiva sempre que o eleitor necessitar, ou solicitar, a facilidade e não tiver registro no seu cadastro eleitoral.

5.4 Considerações sobre as observações realizadas pela Comissão de Avaliação

I. Considerando as evoluções realizadas no desenvolvimento dos sistemas eleitorais no período desde a primeira urna eletrônica especificada em 1995, a complexidade dos componentes individuais, dos subsistemas e sistemas específicos para serem utilizadas em cada etapa do processo eleitoral (preparação, realização e encerramento das eleições), percebe-se que a comunidade da área de tecnologia da informação ainda possui pouca percepção desta realidade.

II. O TPS 2021 mostrou parte deste cenário externo à Justiça Eleitoral por meio das 32 propostas de testes, algumas dimensionadas de forma inexequível no período estabelecido de 5 dias de trabalho.

III. O planejamento do ambiente de trabalho também reflete alguns pontos a considerar, por ambas as partes, de preparar ou solicitar as facilidades necessárias para a realização dos testes. O investigador que tiver uma bancada de trabalho apropriada para a realização dos testes propostos empregará o seu tempo de forma mais eficiente, e caberá à Justiça Eleitoral avaliar a viabilidade da preparação desse ambiente.

IV. Apesar de algumas propostas terem objetivos similares, os perfis técnicos dos investigadores apresentaram abordagens diferenciadas que, a princípio, demonstram uma variedade de abordagens possíveis, em que observou-se o despreparo por conta da falta de informação e tempo para rever e aprimorar os planos de testes.

V. As facilitações realizadas pela equipe técnica de apoio, por solicitação dos investigadores, como, por exemplo, o fornecimento de senhas, dificultou a análise do escopo do teste e dos resultados obtidos, pois não se tem um documento de referência de riscos e avaliações realizadas pela Justiça Eleitoral durante o

desenvolvimento dos sistemas eleitorais e, também, não se tem a certificação para o uso em produção (ambiente real de eleições). A publicidade dos documentos deve estar de acordo com a sua classificação, constante na política de segurança da informação que regulamenta o acesso e a classificação de documentos do Tribunal Superior Eleitoral.

6 Recomendações do TPS 2019

As recomendações contidas no Relatório Final da Comissão Avaliadora do TPS/2019 foram apreciadas pelo TSE e as ações decorrentes relatadas à esta comissão estão enumeradas a seguir.

6.1 Comitê de Assessoria Perene

Recomendação: Instituir um Comitê de Assessoria Perene tendo em vista que os ajustes nos sistemas eleitorais são realizados de forma continuada por conta das atualizações tecnológicas e informes de segurança apresentados, seria recomendável que houvesse uma avaliação técnica acompanhando as decisões de modificações propostas, não se limitando ao evento do TPS. Desta forma, poderia haver uma contribuição mais significativa para as propostas para o TPS.

Resposta do TSE: O TSE não atendeu esta recomendação.

6.2 Reunião virtual e presencial previamente ao TPS

Recomendação: Realizar reunião virtual e presencial previamente ao TPS, bem como após o mesmo, contando com a participação da Comissão Reguladora e dos investigadores. Os investigadores novos no processo necessitam muito tempo para conhecer o sistema eleitoral e os seus componentes (hardware, software e procedimentos). Uma reunião técnica poderia acelerar o processo de esclarecimento, permitindo aos investigadores um conjunto maior de oportunidades para identificar as possíveis vulnerabilidades e elaborar planos mais precisos.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "A Resolução TSE 23.444/2015 já prevê a transmissão de conhecimento aos investigadores no art. 18:
>
> *Art. 18. Na fase de preparação, deverão ser realizadas as seguintes ações ou eventos:*
>
> *...*
>
> *III – palestra informativa sobre o sistema eletrônico de votação com o objetivo de subsidiar os eventuais participantes sobre o funcionamento do sistema eleitoral;*

Alinhados a esse entendimento, foi realizada uma palestra técnica direcionada aos investigadores no dia 11/10/2021 de forma presencial e virtual, com vídeos disponibilizados no hotsite do TPS 2021 a todos os interessados.

Ademais, com a possibilidade de custeio de deslocamento para a fase de inspeção prévia dos códigos-fonte, grande parte dos investigadores esteve em Brasília e teve a possibilidade de sanar eventuais dúvidas diretamente com as equipes técnicas que ficaram à disposição no período de 11 a 22/10/2021."

6.3 Processo de desenvolvimento

Recomendação:

a. implantar processo de desenvolvimento seguro de software (apontado como recomendação já no TPS/2017). O ciclo de vida do desenvolvimento seguro é um processo que consiste na inserção de várias atividades e produtos relacionados à segurança na fase de desenvolvimento de software como modelagem de ameaças, análise estática do código com uso de ferramentas, revisão de código, testes de segurança direcionados e uma revisão final de segurança, minimizando o surgimento de vulnerabilidades.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "Definimos e publicamos uma Norma de Desenvolvimento Seguro, por meio da Portaria n. 540/2021 (em anexo), e estamos adquirindo também uma solução para análise estática de código fonte (por meio do Pregão 58/2021, que se encontra em curso).
>
> Com essas duas ações estamos iniciando a implementação da metodologia de desenvolvimento seguro no TSE. Ainda se faz necessário, entretanto, que as recomendações definidas na norma sejam efetivamente implementadas."

Recomendação:

b. Obter certificados com consultorias independentes e reconhecidas internacionalmente para processo de desenvolvimento seguro de software fará com que o TSE seja publicamente credenciado em práticas adequadas e reconhecidas internacionalmente.

Resposta do TSE: O TSE não atendeu esta recomendação.

Recomendação:

c. Realizar auditorias cientificamente embasadas. Auditorias cientificamente fundamentadas são a base da forense computacional, especialidade de segurança computacional voltada para a verificação do funcionamento esperado de um sistema e da detecção de eventuais comportamentos estranhos ao mesmo, com base nos rastros (não limitados a arquivos de log) que toda execução de software provoca em um sistema computacional, seja em sistemas de arquivos, seja em memórias internas a dispositivos computacionais. Princípio fundamental do processo é o exame de dispositivos de armazenamento não no sistema sob análise, mas sim em sistema de confiança. Semelhantemente, a análise de dispositivos internos deve utilizar o processador do sistema sob análise, mas rodando sistema operacional e utilitários confiáveis, portanto externos ao

mesmo. Em contraste, as rotinas de verificação hoje disponíveis na urna não obedecem a tais princípios.

Resposta do TSE: O TSE atendeu parcialmente esta recomendação, consoante a seguinte informação:

> "Já é permitida esse tipo de auditoria independente dos sistemas da urna desde 2019."

Recomendação:

d. Tornar o exame do software da urna perene e constante, mas mantendo o TPS no formato em que está. Esta comissão entende que o processo de análise e busca de vulnerabilidades devem ser contínuos, com organizações acadêmico científicas que demonstrem competência e disponibilidade de recursos humanos (tipicamente alunos de pós-graduação e pesquisadores experientes). A extensão natural do mesmo seria a disponibilização do código-fonte de forma aberta, entretanto a maioria dos testes exige também o acesso ao hardware, algo que é mais facilmente viabilizado em instituições de ensino e pesquisa. Somente com o aumento do tempo de exposição ao código e entendimento do sistema é que é possível elaborar testes mais complexos que permitam descobrir vulnerabilidades mais sofisticadas. O TPS em si poderia ser utilizado como uma ocasião para demonstração de provas de conceito e troca de experiências entre equipes de investigadores.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "Aumentado o prazo para inspeção do código-fonte dos sistemas na Resolução TSE 23.603/2019:
>
> Art. 8º É garantido, às entidades fiscalizadoras, a partir de 12 (doze) meses antes do primeiro turno das eleições, o acesso antecipado aos sistemas eleitorais desenvolvidos pelo Tribunal Superior Eleitoral e o acompanhamento dos trabalhos para sua especificação e desenvolvimento, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal Superior Eleitoral. (Redação dada pela Resolução nº 23.652/2021)."

6.4 Quanto ao código fonte

Recomendação:

a. Disponibilizar o código fonte dos sistemas eleitorais, objeto deste TPS/2019, para consulta pública logo após a cerimônia de lacração do código. Foi observado que os investigadores dispõem de escasso tempo para familiarizar-se com o código fonte dos sistemas objeto dos testes. Considerando-se que isto pode ser fator determinante do fracasso de planos de ataque, mascarando, assim, o devido diagnóstico da segurança dos sistemas eleitorais e, portanto, gerando falsa sensação de segurança, recomenda-se que as inscrições para o TPS possam ocorrer antes do pleito anterior, possibilitando sua participação nos eventos da abertura dos sistemas das Eleições a partir de 180 dias antes do primeiro turno,

além de permissão de consulta aos códigos fonte nas dependências da unidade da Justiça Eleitoral mais próxima.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "Ações tomadas:
>
> Incluída Resolução de Auditoria e Fiscalização das Eleições de 2020 a possibilidade dos investigadores participarem da lacração dos sistemas para as eleições.
>
> Aumentou o tempo de análise do código-fonte na lacração para o TPS, de uma para duas semanas.
>
> Aumentou o tempo para Acompanhamento da Especificação e Desenvolvimento dos Sistemas Eleitorais para um ano antes das eleições".

Recomendação:

b. Convidar para participar da cerimônia de lacração do código, inclusive colocando suas assinaturas digitais, aqueles investigadores que obtiverem sucesso, ainda que parcial, em algum de seus planos de ataque e que retornarem para verificar e atestar se o problema apontado foi devidamente corrigido.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "Acatado, incluindo na Resolução de Auditoria e Fiscalização das Eleições de 2020."

6.5 Quanto ao processo de inscrição e de seleção

Recomendação:

Realizar levantamento nas redes sociais, antes da abertura das inscrições em cada TPS, questionando se há vulnerabilidades no sistema eleitoral eletrônico para que aqueles que apresentarem razões minimamente consistentes sejam convidados a participar do próximo TPS, pré-vinculando seus planos de ataque ao teor de suas alegações na mídia. Oferecer-se-ia, inclusive, a opção de montagem de grupo com integrantes de sua livre escolha, respeitadas as vedações constantes do edital (idade, nacionalidade etc).

Resposta do TSE: O TSE não atendeu esta recomendação.

6.6 Quanto à ampliação do objeto do TPS

Recomendação:

a. Estender o TPS para testar elementos em maior profundidade, possibilitando a remoção prévia das barreiras existentes de forma a tornar mais acessível o ponto específico dos testes. Em razão do exíguo tempo disponível durante o TPS, para se realizar uma análise

de segurança em profundidade, propõe-se que parte das barreiras de segurança existentes sejam seletivamente removidas, de forma a expor subsistemas mais internos à ação dos investigadores. Como segurança computacional é normalmente obtida com várias camadas ou níveis de profundidade, assim também os testes de segurança deveriam ser capazes de verificar individualmente cada barreira, de forma a que se possa aperfeiçoá-la, independentemente das demais existentes. Um sistema assim aperfeiçoado estará muito mais eficaz para resistir a ataques mais elaborados e complexos, ou seja, aqueles em que os atacantes disponham de mais tempo de análise do sistema-alvo e de preparação do ataque.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "A flexibilização de barreira já é permitida cabendo ao investigador fazer a solicitação que será avaliada do ponto de vista de viabilidade técnica."

Recomendação:

b. Estender o TPS para cobrir não apenas ataques computacionais, mas também ataques de engenharia social. Muitos sistemas computacionais acabam sendo atacados com sucesso justamente através das pessoas que detêm acesso mais privilegiado aos mesmos. Efetivamente são ataques indiretos, contra o que se convenciona chamar o elo mais fraco, no caso as pessoas. A literatura é plena de exemplos de casos assim, sob o nome de *phishing scam* ou *spear phishing*. Trata-se de se desferir ataques que tentam convencer pessoas a involuntariamente executar código estranho malicioso, comprometendo a máquina de um usuário interno à infraestrutura do TSE/TRE e estabelecendo uma "cabeça de ponte" para o atacante elaborar ataques precisos e sofisticados contra alvos internos geralmente desprotegidos das ferramentas usuais de defesa.

Resposta do TSE: O TSE não atendeu esta recomendação.

Recomendação:

c. Ampliar o objeto de testes do TPS, incluindo os sistemas elencados no edital do TPS/2019 Art. 2º §2º incisos I a VII e IX, a saber: identificação e verificação biométrica do eleitor; preparação e infraestrutura para o Kit JE Connect; processamento dos arquivos de urna (fase posterior às fases de transmissão e de recebimento dos arquivos gerados pela urna eletrônica após o encerramento da votação na seção); totalização (TOT) e gerenciamento da totalização (GER); acesso às máquinas servidoras; acesso aos bancos de dados; ataques de negação de serviço; sistema de geração de chaves criptográficas.

Resposta do TSE: O TSE não atendeu esta recomendação.

> O TSE informa que: "Quanto à biometria: Se buscaria evidenciar problemas associados à identificação biométrica quando é inerente à própria tecnologia, como o falso positivo ou falso negativo.
>
> Totalização: Prioridade menor, pois é facilmente auditável e reprodutível a partir do resultado publicado pela urna."

6.7 Quanto ao ambiente de realização do TPS

Recomendação:

a. Organizar as baias e mesas de trabalho dispondo os monitores de forma privativa para os investigadores, em conformidade com os termos de confidencialidade por eles assinados. Os testes devem ser realizados de forma reservada, possibilitando um ambiente mais controlado, o sigilo e a tranquilidade para o seu procedimento, o qual deverá ser acompanhado pela equipe reguladora.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "O ambiente foi projetado para permitir a contribuição entre os investigadores.
>
> Além do mais, na edição deste ano, considerando a ampliação do quantitativo de investigadores e as restrições decorrentes da pandemia de COVID-19, fez-se necessário o desenho de um ambiente aberto."

Recomendação:

b. Melhorar o sistema de registro de solicitação de apoio técnico. Considerar a possibilidade de que a equipe de apoio técnico disponha de *tablets* para abrir videochamadas, ou chats, para que os investigadores prontamente entrem em contato com o responsável técnico. A Comissão Avaliadora deverá ter acesso em tempo real (em meios digitais ou em papel) às solicitações realizadas pelos investigadores e às respectivas respostas.

Resposta do TSE: O TSE atendeu parcialmente esta recomendação, consoante a seguinte informação:

> "A estratégia foi a de manter à disposição do evento quantidade suficiente de técnicos, USP e TSE, para cobrir as eventuais demandas dos investigadores de forma imediata.
>
> Quanto aos documentos para subsidiar a avaliação da comissão avaliadora, manteve-se o encaminhamento das informações sempre que solicitado."

Recomendação:

c. Disponibilizar para Comissão Avaliadora acesso WiFi através de SSID próprio e não pelo SSID TSE-EVENTOS. A estrutura computacional destinada à Comissão Avaliadora deverá estar pronta e disponível com antecedência.

Resposta do TSE: O TSE não atendeu esta recomendação.

Recomendação:

d. Permitir a troca de informação ('*brainstorm*') entre os investigadores para maximizar o potencial criativo. Para tanto, determinar horários específicos para curtos intervalos, com deslocamento físico a ambiente adequado, acompanhados do apoio técnico, que registre tal

intercâmbio e certifique-se de que constem os devidos créditos naqueles planos de ataque que alcancem sucesso com o auxílio de tal intercâmbio.

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "O ambiente do TPS permite a interação entre os investigadores sem restrição de horários."

6.8 Quanto às modificações nos sistemas objeto do TPS

Recomendação:

a. O ataque à cifragem da mídia de armazenamento do sistema GEDAI revelou que a barreira implementada pelo sistema de proteção SIS e de criptografia (TrueCrypt) e o método de armazenamento de chaves não é muito eficaz. Portanto, recomenda-se uma revisão profunda do ambiente operacional e dos mecanismos de proteção necessários para que o GEDAI possa estar instalado de forma segura e confiável para cumprir a sua função de preparação de mídias para a urna eletrônica. Evitar o uso de produtos descontinuados, como é o caso do TrueCrypt, ou aqueles que não estejam validados especificamente e que sejam comprovadamente seguros e confiáveis. As chaves de criptografia devem ser armazenadas usando equipamentos de segurança para armazenamento de chaves, como HSM (Hardware Security Modules).

Resposta do TSE: O TSE atendeu esta recomendação, consoante a seguinte informação:

> "Para o teste de confirmação do TPS 2019 e as eleições de 2020 foi implementado mecanismo de segurança baseado no processador TPM para proteção das chaves utilizadas pelo GEDAI-UE.
>
> No Teste de Confirmação essa solução foi validada e se mostrou robusta."

Recomendação:

b. Diferenciar o som de aviso, emitido durante a inicialização no dia da votação, bem como ao término da votação, e também nos procedimentos que precedem o dia da votação, seja selecionado para um outro distinto do som padrão de aviso emitido quando o eleitor concluir o seu voto. O objetivo é de que a emissão dos referidos avisos de inicialização e término, entre outros, não seja confundida com o aviso de que foi inserido novo voto na urna, visto que a população já assimilou tal som como sendo o de término de inserção do voto.

Resposta do TSE: O TSE atendeu esta recomendação.

Recomendação:

c. Mostrar, no display, aviso de que o cabo do teclado "se desconectou", caso a urna identifique mau contato no cabo do teclado. Contudo, a urna deve continuar inoperante.

Resposta do TSE: O TSE atendeu esta recomendação.

6.9 Publicação do compêndio da documentação

Recomendação:

Publicar, em formato físico e eletrônico, compêndio da documentação produzida e conclusões desta Comissão Avaliadora, conforme disposto no inciso II do artigo 20 da Resolução 23.444/2015 do TSE.

Resposta do TSE: O TSE atendeu parcialmente esta recomendação, consoante a seguinte informação:

> "Acatado parcialmente, não houve impressão."

7 Recomendações TPS 2021

7.1 Documentação das barreiras facilitadas para a execução dos planos

Os testes estão evoluindo a cada etapa identificando que os sistemas eleitorais desenvolvidos estão maduros e seguros quando observados como um sistema, ou subsistema. Os elos entre os subsistemas asseguram a maior parte da segurança e confiabilidade do sistema.

Todavia, quando um subsistema, ou parte dela, é verificada, nota-se a falta de documentação adequada para suportar as decisões técnicas e tecnológicas adotadas.

Ao facilitar as barreiras para que os investigadores possam avançar nos seus planos e intentos, há uma certa dificuldade em entender esse novo ambiente. As respostas fornecidas, ou as solicitações de facilidade atendidas estão ainda fundamentadas nos conhecimentos dos desenvolvedores e suas percepções.

Recomenda-se a revisão, complementação e divulgação desses documentos, para adequar os testes e os planos e garantir os objetivos do TPS de forma mais eficaz.

A existência dos documentos dessa natureza pode contribuir para que os investigadores e os interessados possam focar nas suas propostas e planos de forma consistente com o tempo que o evento proporciona.

7.2 Quanto ao ambiente de realização do TPS

a. Considerando o regulamento que dispõe sobre a segurança física, o acesso ao ambiente e a divulgação dos resultados obtidos pelos investigadores no TPS. e a área preparada para que a imprensa e os observadores externos possam acompanhar o funcionamento do TPS, recomenda-se uma revisão dos espaços utilizados pelos investigadores para prover privacidade aos mesmos em relação ao público externo. O objetivo é a realização dos testes de forma reservada e em ambiente controlado.

b. Considerando que o TPS 2021 teve a equipe de apoio técnico, a qual foi composta pelo corpo acadêmico da USP, é adequado disponibilizar uma bancada com todos os elementos usados no TPS de forma a possibilitar a avaliação e testes operacionais para subsidiar essa equipe técnica com insumos para melhor subsidiar os investigadores.

7.3 Relativo ao modelo distribuído de conexão à rede da JE para envio dos dados de apuração da UE

a. Recomenda-se avaliar adoção de modelo centralizado de conexão dos agentes remotos para facilitar a identificação de tentativas de acesso indevido e manter um registro centralizado de eventos no envio dos dados de apuração provenientes da urnas,;

b. O Transportador continua sendo um item necessário para os agentes remotos. Para evitar *man-in-the-middle*, faz-se necessário uso de um aplicativo no lado do usuário para validação do servidor de aplicação para o qual será enviado os arquivos de apuração (*certificate pinning* ou equivalente). Adicionalmente, o aplicativo continuaria a checar a integridade do arquivo antes de seu envio.

   Ainda, deve-se manter o Módulo Transportador o mais simples possível, sem adição de funcionalidades desnecessárias à sua operação.

c. Avaliar os mecanismos de autenticação, autenticidade e auditoria existentes para acesso ao RecArquivos, imaginando o cenário onde as conexões são oriundas de um elemento na rede interna da JE, ou então no caso em que os boletins de urna e RDVs seriam enviados por fora do JEConnect, sem passar pelas validações no lado cliente;

d. Uso de *token* criptográfico para armazenamento das chaves privadas usadas pelos agentes remotos;

e. Avaliar se o uso de certificado sob a ICP-Brasil como um elemento de autorização no RecArquivos, caso adotado o modelo centralizado, não seria um fator inibidor de comprometimento de agentes internos, tendo em vista que o registro de quem fez o envio do boletim e RDV adulterados ficaria nos logs - *há aqui um ponto de responsabilização que deve ser legalmente analisado*. Algumas considerações devem ser observadas:

e.1 Um dos pontos positivos de uso de certificado ICP-Brasil é que esse modelo facilitaria a logística de distribuição de *tokens*, já que os mesmos estariam de posse dos agentes externos previamente, para uso em outras atividades rotineiras.

e.2 Analisar como operacionalizar a homologação dos agentes remotos que terão acesso ao sistema RecArquivos durante o pleito (portal com duplo fator de autenticação com uso de login/senha e um *token* de autenticação?).

7.4 Dar maior publicidade ao Boletim de Urna com uma revisão da necessidade da criptografia a ele aplicado

a. Considerando que o boletim de urna é divulgado nas seções eleitorais após o encerramento da votação e as cópias distribuídas aos representantes dos partidos políticos presentes e ao comitê interpartidário, não há necessidade em criptografar o boletim de urna, que é a síntese da apuração após a aplicação das regras de contagem legalmente estabelecidas. Todavia, isso será viável somente se a Justiça Eleitoral der ampla divulgação do procedimento realizado na seção eleitoral e também viabilizar a sua distribuição na forma eletrônica. A função da criptografia somente será totalmente substituída pela assinatura digital, que é realizada, facilitando a sua distribuição e verificação.

b. Avaliar a possibilidade do TSE abrir canal de distribuição dos boletins de urna com os partidos e entidades de controle, facilitando a totalização pelos interessados. Não se vê aumento de risco ao processo eleitoral com essa abertura, já que são itens públicos disponíveis de forma impressa nas seções eleitorais após sua apuração, porém é necessário dar ampla divulgação ao público em geral de que ele é um item aberto para que todos os cidadãos possam acompanhar o processo eleitoral.

7.5 Quanto às questões relativas às UE

a. Considerando que os riscos associados a disponibilização do código fonte da UE em plataforma aberta, além das dependências com o hardware para sua operação, podem ser avaliados por meio de estabelecimento de convênios com entidades externas, de amplo espectro e idôneas, incluindo as entidades acadêmicas e de pesquisa;

b. Como uma melhoria no processo de auditoria das UE após o encerramento das eleições na seção eleitoral, recomenda-se um estudo para detecção sistêmica de anomalias na distribuição de votos em zonas onde a comunidade possua um nível socioeconômico equivalente, observando sua posição geográfica, para que essas urnas possam ser utilizadas como objeto de análise.

7.6 Busca por novas abordagens para os desafios do Processo Eleitoral

a. Considerando a evolução tecnológica, tanto em termo de infraestrutura quanto de plataformas/sistemas/algoritmos, sugere-se ao TSE avaliar possibilidade de promover ou participar de eventos como *hackathon* ou DEFCON, para a busca de novas abordagens aos problemas e desafios existentes no processo eleitoral, tais como modelos de detecção de anomalias, disponibilização dos dados de apuração de modo íntegro e auditável a todas as pessoas e entidades que tenham interesse. Visando reunir equipes excepcionais, além da premiação àqueles que obtiverem sucesso em identificar ou causar anomalias no processo eleitoral, sugere-se a criação de um prêmio por excepcionalidade da solução proposta, que é dado de forma discricionária, sem caráter obrigatório. A solução que foi objeto desta premiação deve ter ampla publicidade, com justificativas para embasamento de sua concessão.

8 Considerações Finais

O evento do TPS 2021 apresentou uma equipe técnica capacitada para dar apoio aos investigadores, abrangendo a vasta área de conhecimento técnico e de procedimentos eleitorais. Esse ambiente proporciona respostas em tempo adequado para que os investigadores pudessem dominar, a cada dia do evento, as características inerentes dos processos e sistemas eleitorais, adequando os seus planos e avançando nos trabalhos. O tempo de exposição dos investigadores nesse tipo de ambiente é reduzido, mas adequado aos objetivos do TPS (exposição dos sistemas no período compreendido entre o preparo e a realização das eleições).

Observa-se ao longo dos eventos do TPS realizados de 2009 até o momento, que os resultados apresentados demonstram a maturidade dos sistemas eleitorais. Todavia, nota-se, em alguns testes, que os avanços obtidos pelos investigadores demonstram também a relevância dos subsistemas e componentes, que isoladamente, ainda apresentam espaços para a sua melhoria nos quesitos relativos à qualidade do projeto e a dependência dos mecanismos de segurança externos ao mesmo (riscos internos e externos).

O retorno de alguns investigadores para verificar as correções e os ajustes realizados pela equipe técnica da Justiça Eleitoral será um momento importante para registrar o início dos preparativos operacionais das eleições de 2022.

A publicação da Portaria nº 540, de 23 de agosto de 2021, do TSE, que dispõe sobre a instituição da Norma de Desenvolvimento Seguro de Sistemas, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral, renova o conjunto de documentos que regulamenta os desenvolvimentos realizados até o momento e acrescentará, com certeza, aperfeiçoamentos procedimentais e tecnológicos em consonância com as ameaças modernas. Acredita-se que os quesitos de análise de cada caso de desenvolvimento e

emprego dos mecanismos de segurança e as respectivas documentações serão atendidos até a realização das eleições gerais de 2022.

A análise dos processos, sistemas, subsistemas e componentes, avaliados continuamente de acordo com o cenário dinâmico de candidaturas, campanhas e divulgação de informações eleitorais garantirão a capacidade de rever os riscos de forma consistente, transmitindo a segurança e a confiabilidade aos eleitores para terem a certeza do valor do seu voto realizado, amparado pela Justiça Eleitoral.