Relatório da Comissão Avaliadora

Primeira Etapa do TPS 2023

Realização: 27 de novembro a 02 de dezembro de 2023

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 701, de 20 de setembro de 2023, 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, composta por 13 membros, contou nesta segunda etapa com a presença dos representantes dos seguintes órgãos:

- TSE - Rogério Marrone de Castro Sampaio - Juiz Auxiliar da Presidência;
- TSE - Paulo Rogério Bonini - Juiz Auxiliar da Presidência;
- Membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:
    - Jamil Salem Barbar - Professor Doutor;
    - Mamede Lima-Marques - Professor Doutor;
    - Osvaldo Catsumi Imamura - Professor Doutor;
    - Antônio Esio Marcondes Salgado - Professor Mestre;
- MPF - Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas;
- CFOAB - Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico;
- CN - Veneziano Vital do Rêgo - Senador da República;
- PF - Paulo César Herrmann Wanner - Perito Criminal Federal e Coordenador da CCAT/CGCIBER/DCIBER/PF;
- TCU - André Luiz Furtado Pacheco - Auditor Federal de Controle Externo;

- CONFEA - Rodrigo de Souza Borges - Engenheiro de Computação e Gerente de Tecnologia da Informação;
- SBC - Roberto Samarone dos Santos Araújo - Professor Doutor.

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

2 Metodologia de Avaliação dos Testes

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

- Não executados;
- Executados sem contribuição para melhoria do sistema;
- Executados com contribuição para melhoria do sistema.

3 Planos de Teste Aprovados

A Comissão Reguladora aprovou 34 planos e os objetos das propostas foram os seguintes:

1. Plano de Teste 01:
   - Título: Quebra do sigilo do voto
   - Investigador(es): Aline Barbosa da Silva Ferreira
   - Resumo do teste: No dia da Eleição, a votação se inicia normalmente. O primeiro eleitor vota, assim sucessivamente irei retirar da urna eletrônica a mídia de resultados. Ela será lida no Notebook com o kit JE-Connect, assim quebrando o sigilo do voto do eleitor.
2. Plano de Teste 02:
   - Título: Fragilizar sigilo do voto
   - Investigador(es): Aline Barbosa da Silva Ferreira
   - Resumo do teste: No dia da Eleição na seção de votação, irei instalar um dispositivo na urna eletrônica em que ao eleitor pressionar as teclas do seu voto, o dispositivo emitira o som de qual tecla foi acionada.
3. Plano de Teste 03:
   - Título: Invadir a mídia de carga da urna eletrônica
   - Investigador(es): Aline Barbosa da Silva Ferreira

- **Resumo do teste**: Invadir a mídia de carga da Urna Eletrônica, fazendo a limitação de votos aos candidatos daquela seção.

4. Plano de Teste 04:
   - **Título**: Inconsistência de Software
   - **Investigador(es)**: Avelino Francisco Zorzo
   - **Resumo do teste**: Executar a avaliação de que o software que foi salvo na urna eletrônica é o mesmo software lacrado em cerimônia pública.
5. Plano de Teste 05:
   - **Título**: Sigilo e proteção do voto: Fortaleza magnética e defesa eletroacústica para a democracia
   - **Investigador(es)**: Diego Ferry Torrent
   - **Resumo do teste**: Resiliência cibernética abordando magnetismo, acústica, ultrassom e escudo faraday saltando a segurança Air-Gapped.
6. Plano de Teste 06:
   - **Título**: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
   - **Investigador(es)**: André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho
   - **Resumo do teste**: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.
7. Plano de Teste 07:
   - **Título**: Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia
   - **Investigador(es)**: Érika Maria Rodrigues de Castro
   - **Resumo do teste**: Trata-se de análise do comportamento da Mídia de Resultado “pen drive” da Urna Eletrônica em algumas etapas.
8. Plano de Teste 08:
   - **Título**: *Fraus omnia corrumpit*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**: Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do eleitor e com isso alterar a disposição dos votos.

9. Plano de Teste 09:
   - Título: *Nihil autem absconditum est, quod non reveletur*
   - Investigador(es): Guilherme Henrique dos Santos
   - Resumo do teste: Obter o conteúdo do RDV em mídia alternativa, inserir em urna de contingência, e a partir da comparação da diferença entres os arquivos e da ordem de eleitores habilitados violar o sigilo do voto.
10. Plano de Teste 10:
   - Título: *Qui duplicat, videre suffragio potest*
   - Investigador(es): Guilherme Henrique dos Santos
   - Resumo do teste: Violar sigilo do voto, a partir da sequência de votantes e do conteúdo obtido do *display* do terminal de eleitor com acoplamento de um *Splitter* na saída de vídeo e outro display.
11. Plano de Teste 11:
   - Título: *Suffragium simulata substantiam veritas mutare possunt*
   - Investigador(es): Guilherme Henrique dos Santos
   - Resumo do teste: Alterar a destinação dos votos, substituindo a votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.
12. Plano de Teste 12:
   - Título: Violar a confidencialidade, integridade e disponibilidade das informações no *Python* do Software JE-Connect
   - Investigador(es): Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
   - Resumo do teste: A linguagem de programação *Python* apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo *Python* usa a função str.format e string-f na formatação de *string*. Essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.
13. Plano de Teste 13:
   - Título: Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do *Python* para geração de arquivos XML no Software JE-Connect
   - Investigador(es): Prof. Dr. Carlos Alberto da Silva; Ian Martinez Zimmermann; Matheus Vianna Silveira; Mario de Araújo Carvalho

- **Resumo do teste**: Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, onde um invasor pode abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas ou contornar firewalls.

14. Plano de Teste 14:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JE-Connect
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: A função urllib.parse na linguagem de programação *Python* possui uma falha de segurança de alta gravidade na função de análise de URL do *Python*, que pode ser explorada para ignorar os métodos de filtragem de domínio ou protocolo implementados com uma lista de bloqueio, resultando em leituras arbitrárias de arquivos e execução de comandos.
15. Plano de Teste 15:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JE-Connect
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Executar um *exploit* funcional que permite chamar qualquer comando do sistema sem acesso direto a métodos como os.system. Este *exploit* é implementado em Python puro, e funciona sem importar bibliotecas externas, e sem instalar o driver "code.__new__".
16. Plano de Teste 16:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JE-Connect
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Executar vários *exploits* funcionais para permitir chamadas de: comandos e funções as bibliotecas nativas e externas do Python, e obter acesso as informações.
17. Plano de Teste 17:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita

- **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araujo Carvalho
- **Resumo do teste**: Executar vários *exploits* funcionais para permitir chamadas de: comandos e obter acesso às informações, com escalada de privilégio.

18. Plano de Teste 18:
    - **Título**: Extração, Verificação e Validação do Conjunto Completo dos Resumos Criptográficos HASH SHA-512 *Radix* 64 dos Códigos Compilados e/ou Executáveis Embarcados na Urna Eletrônica
    - **Investigador(es)**: Prof. Dr. João Benedito dos Santos Junior
    - **Resumo do teste**: Este Plano de Teste está inserido no contexto da verificação de integridade e autenticidade de sistemas eleitorais. Pretende-se, em tempo real, extrair, verificar e validar o conjunto completo dos resumos criptográficos HASH SHA-512 *Radix* 64 dos códigos compilados e/ou executáveis que estiverem embarcados na Urna Eletrônica, considerando um cenário em que seja necessário verificar a integridade e autenticidade após os procedimentos de certificação e liberação das Urnas Eletrônicas para o Pleito Eleitoral.
19. Plano de Teste 19:
    - **Título**: Auditoria de Integridade e Segurança na Apuração Eletrônica de Votos
    - **Investigador(es)**: João Vitor Santana Silva
    - **Resumo do teste**: Teste verifica integridade da apuração de votos para garantir resultados eleitorais confiáveis.
20. Plano de Teste 20:
    - **Título**: Tentativa de *Man-in-the-Middle* na Comunicação do Teclado com Arduíno
    - **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
    - **Resumo do teste**: A avaliação tem como propósito testar vulnerabilidades na comunicação entre o teclado e a placa mãe das urnas.
21. Plano de Teste 21:
    - **Título**: Tentativa de reconhecimento das teclas digitadas usando IA
    - **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves

- **Resumo do teste**: O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identificar as teclas usando um modelo de rede neural, quebrando o sigilo dos votos.

22. Plano de Teste 22:
    - **Título**: USBExploit – acesso a dados da urna através da porta USB
    - **Investigador(es)**: Marcos Roberto dos Santos, Rafael Noll da Silva Eduardo Bido, Rhayara Rodrigues Fiorentin
    - **Resumo do teste**: Captura de informações da urna através da conexão de um cabo console ou adaptador USB que possibilite acesso a dados.
23. Plano de Teste 23:
    - **Título**: Executar código espúrio na Urna Eletrônica modelo 2020
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
24. Plano de Teste 24:
    - **Título**: Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020
    - **Investigador(es)**: Galileu Batista de Sousa
    - **Resumo do teste**: Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
25. Plano de Teste 25:
    - **Título**: Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Caso seja possível extrair a chave que cifra/decifra o kernel da urna, uma chave derivada dessa poderá ser utilizada para cifrar um RDV falso. Posteriormente esse RDV falso poderia ser carregado em uma urna de contingência.
26. Plano de Teste 26:
    - **Título**: Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI

- **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- **Resumo do teste**: Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.

27. Plano de Teste 27:
    - **Título**: Alterar dados / programas nos sistemas SIS/GEDAI
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Utilizando técnicas de análise de código/engenharia reversa, e se necessário algum hardware de apoio, comprometer o funcionamento adequado dos sistemas SIS / GEDAI de modo a propagar informações falsas entre os sistemas e a Urna Eletrônica, ou mesmo não propagar informação alguma.
28. Plano de Teste 28:
    - **Título**: Ataque de *cold boot* à Urna Eletrônica
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Congelamento da memória RAM da urna, objetivando extrair os dados em leitor externo para posterior decodificação.
29. Plano de Teste 29:
    - **Título**: Execução do JE-Connect utilizando computador com sistema operacional inválido
    - **Investigador(es)**: Nicholas Barros dos Santos
    - **Resumo do teste**: Analisar a eficácia da execução do JE-Connect em computadores que apresentam falhas na validação do sistema operacional.
30. Plano de Teste 30:
    - **Título**: Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados
    - **Investigador(es)**: Nicholas Barros dos Santos
    - **Resumo do teste**: Analisar o comportamento do JE-Connect em um computador na execução de um *bot*, para atestar a sua integralidade na transmissão de dados.
31. Plano de Teste 31:
    - **Título**: Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de *shell* a partir de um dispositivo USB

- **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili; Brayan Vanz de Oliveira
- **Resumo do teste**: Abertura de um *shell* no sistema operacional responsável pela comunicação JE-Connect para obter acesso a rede do TSE.

32. Plano de Teste 32:
    - **Título**: Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores
    - **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili; Brayan Vanz de Oliveira
    - **Resumo do teste**: Abrir a Urna e substituir o cabo HDMI para outro cabo que possua um dispositivo, o qual remeta a imagem para outro dispositivos conectados via Bluetooth.
33. Plano de Teste 33:
    - **Título**: Investigação dos mecanismos de validação do *bootloader* pela BIOS para a proteção da carga segura do SO da UE
    - **Investigador(es)**: Ricardo Antônio Pralon Santos
    - **Resumo do teste**: Investigação dos meios de proteção do *bootloader* da UE e a possibilidade de substituição por um *bootloader* "malicioso".
34. Plano de Teste 34:
    - **Título**: Adulteração no JE-Connect
    - **Investigador(es)**: Vitor Aloisio do Nascimento Guia, Hitatiana Maria Santiago Ferreira da Silva Guia
    - **Resumo do teste**: Garantir que não seja possível obter privilégios de usuário root na *distro* Linux do MSE de forma a adulterar o JEC.
35. Plano de Teste 35*[1]:
    - **Título**: Teste de escalação de privilégios no Windows (SIS)
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Utilizar falha de permissão para escalar privilégio e acesso a arquivos críticos.

[1] *Planos de Teste Adicionais solicitados no transcorrer do TPS (35 a 38)

36. Plano de Teste 36*:
    - Título: *Ab initio in valid post valid*
    - Investigador(es): Guilherme Henrique dos Santos
    - Resumo do teste: Alterar a tabela de correspondência.
37. Plano de Teste 37*:
    - Título: *Omnia invalid est*
    - Investigador(es): Guilherme Henrique dos Santos
    - Resumo do teste: Usar o SA como validador de um BU com votos inválidos.
38. Plano de Teste 38*:
    - Título: *Suffragium non est relatus*
    - Investigador(es): Guilherme Henrique dos Santos
    - Resumo do teste: Descarte de votos mediante substituição por um período de tempo da MV (Mídia de Votação) por uma MV clonada.

4 Planos de Teste Executados

Para tornar os trabalhos de avaliação consistentes com o andamento das investigações e com os registros efetuados pela Equipe de Apoio Técnico do TPS 2023, constituída para acompanhar as atividades, registra-se a seguir os planos efetivamente executados pelos 16 grupos formados durante os testes.

1. Grupo 1:
    - Título(s): Quebra do sigilo do voto; fragilizar sigilo do voto; invadir a mídia de carga da urna eletrônica
    - Investigador(es): Aline Barbosa da Silva Ferreira
    - Resumo do teste:
        1. No dia da Eleição, a votação se inicia normalmente. O primeiro eleitor vota, assim sucessivamente irei retirar da urna eletrônica a mídia de resultados. Ela será lida no Notebook com o kit JE-Connect, assim quebrando o sigilo do voto do eleitor.
        2. No dia da Eleição na seção de votação, irei instalar um dispositivo na urna eletrônica em que ao eleitor pressionar as teclas do seu voto, o dispositivo emitira o som de qual tecla foi acionada.

3. Invadir a mídia de carga da Urna Eletrônica, fazendo a limitação de votos aos candidatos daquela seção.

- **Plano de Teste Proposto**: 1, 2 e 3.

2. Grupo 2:
   - **Título(s)**: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
   - **Investigador(es)**: André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho
   - **Resumo do teste**: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.
   - **Plano de Teste Proposto**: 6
3. Grupo 3:
   - **Título(s)**: Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia
   - **Investigador(es)**: Érika Maria Rodrigues de Castro
   - **Resumo do teste**: Em resumo: trata-se de Trata-se de análise do comportamento da Mídia de Resultado "pen drive" da Urna Eletrônica em algumas etapas
   - **Plano de Teste Proposto**: 7
4. Grupo 4:
   - **Título(s)**: *Fraus omnia corrumpit; nihil autem absconditum est, quod non reveletur; qui duplicat, videre suffragio potest; suffragium simulata substantiam veritas mutare possunt, Ab initio in valid post valid, Omnia invalid est, Suffragium non est relatus*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**:
     1. Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do eleitor e com isso alterar a disposição dos votos.
     2. Obter o conteúdo do RDV em mídia alternativa, inserir em urna de contingência, e a partir da comparação da diferença entres os arquivos e da ordem de eleitores habilitados violar o sigilo do voto.
     3. Violar sigilo do voto, a partir da sequência de votantes e do conteúdo obtido do display terminal de eleitor com acoplamento de um Splitter na saída de vídeo e outro display.

4. Alterar a destinação dos votos, substituindo a votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.
5. Alterar a tabela de correspondência.
6. Usar o SA como validador de um BU com votos inválidos.
7. Descarte de votos mediante substituição por um período de tempo da MV (Mídia de Votação) por uma MV clonada.

- Plano de Teste Proposto: 8. 9. 10, 11, 36, 37 e 38

5. Grupo 5:

- Título(s): Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita.
- Investigador(es): Prof. Dr. Carlos Alberto da Silva; Ian Martinez Zimmermann; Matheus Vianna Silveira; Mario de Araujo Carvalho
- Resumo do teste:
    1. A linguagem de programação Python apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo Python usa a função str.format e string-f na formatação de string. essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.
    2. Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, onde um invasor pode abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas ou contornar firewalls.
    3. A função urllib.parse na linguagem de programação Python possui uma falha de segurança de alta gravidade na função de análise de URL do Python, que pode ser explorada para ignorar os métodos de filtragem de domínio ou protocolo implementados com uma lista de bloqueio, resultando em leituras arbitrárias de arquivos e execução de comandos.

4. Executar um *exploit* funcional que permite chamar qualquer comando do sistema sem acesso direto a métodos como os.system. Este *exploit* é implementado em Python puro, e funciona sem importar bibliotecas externas, e sem instalar o driver "code.__new__".
5. Executar vários *exploits* funcionais para permitir chamadas de: comandos e funções as bibliotecas nativas e externas do Python, e obter acesso as informações.
6. Executar vários *exploits* funcionais para permitir chamadas de: comandos e obter acesso às informações, com escalada de privilégio.

- **Plano de Teste Proposto**: 12, 13, 14, 15, 16, 17 e 35

6. Grupo 6:
   - **Título(s)**: Extração, Verificação e Validação do Conjunto Completo dos Resumos Criptográficos HASH SHA-512 *Radix* 64 dos Códigos Compilados e/ou Executáveis Embarcados na Urna Eletrônica
   - **Investigador(es)**: Prof. Dr. João Benedito dos Santos Junior
   - **Resumo do teste**: Este Plano de Teste está inserido no contexto da verificação de integridade e autenticidade de sistemas eleitorais. Pretende-se, em tempo real, extrair, verificar e validar o conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis que estiverem embarcados na Urna Eletrônica, considerando um cenário em que seja necessário verificar a integridade e autenticidade após os procedimentos de certificação e liberação das Urnas Eletrônicas para o Pleito Eleitoral.
   - **Plano de Teste Proposto**: 18
7. Grupo 7:
   - **Título(s)**: Tentativa de *Man-in-the-Middle* na Comunicação do Teclado com Arduíno; Tentativa de reconhecimento das teclas digitadas usando IA
   - **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
   - **Resumo do teste**:
     1. A avaliação tem como propósito testar vulnerabilidades na comunicação entre o teclado e a placa mãe das urnas.
     2. O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identifica usando um modelo de rede neural, quebrando o sigilo dos votos.
   - **Plano de Teste Proposto**: 20 e 21

8. Grupo 8:

   - **Título(s)**: USBExploit – acesso a dados da urna através da porta USB
   - **Investigador(es)**: Marcos Roberto dos Santos; Eduardo Bido; Rhayra Rodrigues Fiorentin; Rafael Nollda Silva
   - **Resumo do teste**:

     Captura de informações da urna através da conexão de um cabo console ou adaptador USB que possibilite acesso a dados
   - **Plano de Teste Proposto**: 22

9. Grupo 9:

   - **Título(s)**: Executar código espúrio na Urna Eletrônica modelo 2020; Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020; Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto; Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI; Alterar dados / programas nos sistemas SIS/GEDAI; Ataque de cold boot à Urna Eletrônica
   - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
   - **Resumo do teste**:

     1. Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
     2. Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
     3. Caso seja possível extrair a chave que cifra/decifra o kernel da urna, uma chave derivada dessa poderá ser utilizada para cifrar um RDV falso. Posteriormente esse RDV falso poderia ser carregado em uma urna de contingência.
     4. Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.
     5. Utilizando técnicas de análise de código/engenharia reversa, e se necessário algum hardware de apoio, comprometer o funcionamento adequado dos sistemas SIS / GEDAI de modo a propagar informações falsas entre os sistemas e a Urna Eletrônica, ou mesmo não propagar informação alguma.

6. Congelamento da memória RAM da urna, objetivando extrair os dados em leitor externo para posterior decodificação.

- **Plano de Teste Proposto**: 23, 24, 25, 26, 27 e 28

10. Grupo 10:

- **Título(s)**: Execução do JE-Connect utilizando computador com sistema operacional inválido; Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados
- **Investigador(es)**: Nicholas Barros dos Santos
- **Resumo do teste**:

1. Analisar a eficácia da execução do JE-Connect em computadores que apresentam falhas na validação do sistema operacional.
2. Analisar o comportamento do JE-Connect em um computador na execução de um *bot*, para atestar a sua integralidade na transmissão de dados.

- **Plano de Teste Proposto**: 29 e 30

11. Grupo 11:

- **Título(s)**: Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de *shell* a partir de um dispositivo USB; Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores
- **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili, Brayan Vanz de Oliveira
- **Resumo do teste**: 1) Abertura de um *shell* no sistema operacional responsável pela comunicação JE-Connect para obter acesso a rede do TSE. 2) Abrir a Urna e substituir o cabo HDMI para outro cabo que possua um dispositivo, o qual remeta a imagem para outro dispositivos conectados via Bluetooth.
- **Plano de Teste Proposto**: 31 e 32

12. Grupo 12:

- **Título(s)**: Adulteração no JE-Connect
- **Investigador(es)**: Vitor Aloisio do Nascimento Guia, Hitatiana Maria Santiago Ferreira da Silva Guia
- **Resumo do teste**: Garantir que não seja possível obter privilégios de usuário root na *distro* Linux do MSE de forma a adulterar o JEC
- **Plano de Teste Proposto**: 34

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 execução dos planos são apresentados a seguir:

5.1 Planos de teste não executados

Os planos de testes não executados foram: 25, 27 e 28.

5.2 Planos de teste executados sem contribuições

Os planos de teste executados que não obtiveram sucesso no alcance dos objetivos propostos foram: 01, 02, 03, 07, 08, 09, 10, 11, 13, 14, 15, 16, 17, 18, 20, 22, 29, 30, 31, 32, 34, 36, 37 e 38.

Avaliação: As propostas de testes apresentadas encontraram barreiras e proteções que dificultaram o alcance dos objetivos planejados. Todavia, muitos investigadores compareceram com conhecimento e informações insuficientes, necessitando de muito tempo para conseguirem reanalisar os planos de testes e validar os procedimentos planejados, ou buscar alternativas.

5.3 Planos de teste executados com contribuição

Os planos de teste que apresentaram resultados de avanço nos objetivos propostos foram: 06, 12, 21, 23, 24, 26 e 35.

Plano de Teste 06:

- Título: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
- Investigador(es): André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho
- Resumo do teste: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.
- Resultado obtido: O MSTE, Módulo de Segurança do Teclado do Eleitor, não registra os comandos das teclas quando duas teclas são acionadas simultaneamente. Todavia, o acionamento de uma terceira tecla é aceito.

Avaliação: A observação informada não afeta a condução do voto pelo eleitor. Todavia, o conceito de múltiplas teclas estar limitada a somente duas pode ser revisto.

Plano de Teste 12:

- Título: Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JE-Connect
- Investigador(es): Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
- Resumo do teste: A linguagem de programação Python apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo Python usa a função str.format e string-f na formatação de *string*. Essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.
- Resultado obtido: Foi verificado que o sistema JE-Connect realiza o reboot a cada três tentativas de erros de login. Todavia, a reinicialização é invocada de forma simples, permitindo que o usuário a interrompa e retorne à situação de solicitação de login e com o contador de tentativas zerado. Esta ação permite que novas tentativas possam ser realizadas, praticamente sem o limite estabelecido pelo sistema.

Avaliação: A falha no sistema de controle de acesso explorada neste teste deve ser revista e corrigida pois representa uma vulnerabilidade nos conceitos aplicados ao projeto do software. Apesar do impacto no ponto explorado ser reduzido e não comprometer a condução e os resultados das eleições, pode ser uma falha de concepção, recomenda-se uma análise mais abrangente.

Plano de Teste 21:

- Título: Tentativa de reconhecimento das teclas digitadas usando IA
- Investigador(es): Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
- Resumo do teste: O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identificar as teclas usando um modelo de rede neural, quebrando o sigilo dos votos.
- Resultado obtido: Foi obtido uma acurácia de 70% no reconhecimento do acionamento de uma tecla por meio da captação do som emitido pela urna e capturado usando um microfone para um mesmo modelo de urna. A acurácia média diminui para 50% considerando diferentes modelos de urna e posições variadas do microfone. Os resultados obtidos podem ser melhorados com o aprimoramento do algoritmo e uso de recursos computacionais emergentes.

Avaliação: O teste pode ser considerado uma contribuição para o aprimoramento dos componentes da urna eletrônica, na fase de desenvolvimento. O seu emprego em uma seção

eleitoral é impraticável dadas as condições que este ambiente apresenta, tais como ruídos, para a captura dos sinais necessários e processamento da informação.

Plano de Teste 23:

- Título: Executar código espúrio na Urna Eletrônica modelo 2020
- Investigador(es): Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- Resumo do teste: Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
- Resultado obtido: Foi verificado a existência de uma falha no BIOS da urna permitindo a abertura de uma janela de oportunidade para alteração de informação durante a execução do *bootloader*. A verificação da falha foi executada com a carga de uma mensagem não prevista exibida na tela da urna durante a inicialização.

Avaliação: A janela de ataque explorada foi entre a execução da inicialização da urna, um *bootloader* controlado pelo MSE, Módulo de Segurança Embarcado, mas com um coadjuvante que é o programa de carga do BIOS/UEFI, um módulo que controla o funcionamento básico da urna. É um ataque complexo, de um grau de realização baixo por conta dos mecanismos de segurança implementados, mas que deve ser tratado adequadamente para mitigar os riscos apresentados.

Plano de Teste 24:

- Título: Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020
- Investigador(es): Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- Resumo do teste: Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
- Resultado obtido: Foi explorado um comportamento não previsto nos procedimentos de carga controlados pelo BIOS/UEFI e *bootloader*, permitindo a geração de chave para decifração de um bloco do kernel do sistema operacional da urna carregado durante a inicialização.

Avaliação: Uma intervenção do tipo TOCTOU sobre o *bootloader* permitindo o acesso ao processo de entrega da semente para a geração de chave criptográfica deve ser analisada e corrigida. De acordo com a documentação do software, esta janela não deveria existir, mas não está declarada de forma explícita nos requisitos de implementação e no modelo desenvolvimento de software seguro. Assim, recomendamos uma análise dos documentos que originam os requisitos de desenvolvimento e que norteiam a codificação e os testes de conformidade.

Plano de Teste 26:

- Título: Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI
- Investigador(es): Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- Resumo do teste: Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.
- Resultado obtido: Foi obtido as chaves que protegem a partição protegida pelo *Bitlocker* (sistema de proteção nativa do Windows) e ter acesso à área onde ficam residentes o SIS e os sistemas eleitorais a serem carregados na urna.

Avaliação: O sistema de geração de mídias de carga da urna eletrônica é executado em um ambiente protegido pelo SIS e pelo Windows. O resultado obtido neste teste mostra a vulnerabilidade da primeira camada (Windows) que, apesar de não comprometer a segunda camada (SIS), demonstra os riscos associados ao modelo de segurança adotado. Recomenda-se uma nova análise de riscos para o aprimoramento dos conceitos adotados neste domínio.

Plano de Teste 35*:

- Título: Teste de escalação de privilégios no Windows (SIS)
- Investigador(es): Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
- Resumo do teste: Utilizar falha de permissão para escalar privilégio e acesso a arquivos críticos.
- Resultado obtido: Por meio de um acesso a uma conta com baixos privilégios no SIS, foi possível localizar um *endpoint* na aplicação VAP, Verificador de Autenticação de Programas, que permite a elevação de privilégios de leitura e escrita possibilitando o acesso e a edição de arquivos internos do sistema.

Avaliação: Um aplicativo que é executado com determinados privilégios, acima de uma conta comum, deve estar protegido de forma a manter todas as regras de segurança previstas consistentes. Recomenda-se uma análise da questão apresentada para que o processo seja revisto e mantido consistente com os privilégios propostos, evitando eventos não previstos que possam obstruir os procedimentos planejados e projetados. O conceito aplicado para empregar os processos "*open protection*" e "*close protection*" em ambientes hostis necessita ser revisto.

5.4 Considerações sobre as observações realizadas pela Comissão de Avaliação

O TPS 2023 apresentou um cenário mais abrangente que os demais eventos anteriores, em especial pela maior abrangência dos cenários de testes.

A complexidade dos sistemas e dos processos eleitorais foi constatada pela dificuldade que muitos investigadores tiveram em se situar e dominar os seus cenários de testes.

Os resultados alcançados também refletem esta complexidade sistêmica, mas conseguindo demonstrar algumas fragilidades em contextos mais específicos, mas relevantes.

Consequentemente, ainda que esses resultados alcançados pelos investigadores não comprometam a integridade, o sigilo do voto e o resultado das eleições, os riscos associados podem obstruir a boa e natural execução da eleição e merecem ser analisados, os riscos devidamente identificados e os processos consistentes com as evidências apresentadas.

A Comissão avaliadora recomenda que os investigadores dos seguintes testes sejam convidados para uma nova verificação dos achados e das soluções propostas: 12, 23, 24, 26 e 35.