#SEUVOTO TEMPODER
ELEIÇÕES 2020

Tribunal Superior Eleitoral

TPS 2019

TESTE PÚBLICO DE SEGURANÇA

Compêndio

Brasília
TSE
2020

#SEUVOTO TEMPODER
ELEIÇÕES 2020

Tribunal Superior Eleitoral

TPS 2019
TESTE PÚBLICO DE SEGURANÇA

Compêndio

Brasília
TSE
2020

Secretaria de Gestão da Informação
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70070-600
Telefone: (61) 3030-9225

Secretária-Geral da Presidência
Aline Rezende Perez Osorio

Diretor-Geral da Secretaria do Tribunal
Rui Moreira de Oliveira

Secretário de Gestão da Informação
Cleber Schumann

Coordenador de Editoração e Publicações
Washington Luiz de Oliveira

Unidade responsável
Comissão Reguladora do TPS 2019

Editoração e revisão editorial
Coordenadoria de Editoração e Publicações (Cedip/SGI)

Editoração
Seção de Editoração e Programação Visual (Seprov/Cedip/SGI)

Capa e projeto gráfico
Pedro Henrique Silva

Revisão editorial
Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGI)
Gabriela Silva, Paula Lins e Sérgio Félix

Impressão e acabamento
Seção de Serviços Gráficos (Segraf/Cedip/SGI)

Dados Internacionais de Catalogação na Publicação (CIP)
Tribunal Superior Eleitoral – Biblioteca Professor Alysson Darowish Mitraud

Brasil. Tribunal Superior Eleitoral.

TPS 2019 [recurso eletrônico] : teste público de segurança : compêndio / Tribunal Superior Eleitoral. – Dados eletrônicos (163 páginas). – Brasília : Tribunal Superior Eleitoral, 2020.

Ao alto do título: #SeuVotoTemPoder. Eleições 2020.

Unidade responsável: Comissão Reguladora do TPS 2019, Tribunal Superior Eleitoral.

Versão PDF.

Modo de acesso: tse.jus.br/o-tse/catalogo-de-publicacoes/lista-do-catalogo-de-publicacoes

Disponível, também, em formato impresso.

1. Votação – Teste público de segurança – Brasil. 2. Urna eletrônica – Segurança – Brasil. 3. Segurança do voto na urna eletrônica – Brasil. I. Título.

CDD 324.650 981
CDU 342.843.5(81)

Bibliotecária: Sabrina Ruas Lopes – CRB-1/1865

TRIBUNAL SUPERIOR ELEITORAL

Presidente
Ministro Luís Roberto Barroso

Vice-Presidente
Ministro Edson Fachin

Ministros
Ministro Alexandre de Moraes
Ministro Luis Felipe Salomão
Ministro Mauro Campbell Marques
Ministro Tarcisio Vieira de Carvalho Neto
Ministro Sérgio Banhos

Procurador-Geral Eleitoral
Augusto Aras

Sumário

Apresentação

O Teste Público de Segurança (TPS) chegou à sua quinta edição com o objetivo de identificar vulnerabilidades relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Na prática, o Tribunal Superior Eleitoral (TSE) disponibiliza os sistemas eleitorais para que os investigadores e a comunidade técnico-científica, durante o evento, tentem quebrar as barreiras de segurança do processo de votação. Com isso, a Justiça Eleitoral busca o aprimoramento dos mecanismos de segurança do *software* e do *hardware*, contando com a visão e com a experiência de um grande número de pesquisadores e de profissionais altamente qualificados.

A edição do TPS 2019 contou com prazo maior. Até 2017, o cronograma trazia um dia de preparação, três dias de teste e um dia de prorrogação, a pedido. Em 2019, foram realizados cinco dias de teste, e os investigadores deram início aos seus planos de ataque desde o primeiro dia.

Além disso, o teste contou com a participação de um time de observadores formado por secretários da área de Tecnologia da Informação dos Tribunais Regionais Eleitorais (TREs) de Goiás, do Espírito Santo, da Paraíba, do Paraná e de Roraima, que acompanharam de perto os passos dos investigadores durante a execução dos ataques.

Servidores dos TREs de Minas Gerais, do Pará, de Santa Catarina e da Paraíba, especialistas em Segurança da Informação, também participaram do evento, registrando as ações realizadas pelos participantes durante a execução dos planos de teste.

O TPS tornou-se um dos marcos para aprimorar constantemente os sistemas eleitorais com *hardwares* cada vez mais seguros e robustos, além de propiciar confiabilidade, transparência e segurança dos votos.

1. Introdução

O Teste Público de Segurança (TPS), evento inédito no mundo, foi criado por iniciativa do Tribunal Superior Eleitoral (TSE), com o objetivo de fortalecer a confiabilidade, a transparência, a segurança da captação e da apuração dos votos, bem como de propiciar melhorias contínuas no processo eleitoral brasileiro.

Pautado na transparência institucional – um dos pilares de atuação do TSE e de toda a Justiça Eleitoral brasileira –, o teste reúne especialistas em Tecnologia e Segurança da Informação de diversas organizações, instituições acadêmicas e órgãos públicos. Na ocasião, os participantes tentam atacar a urna e seus componentes internos e externos, com o objetivo de descobrir vulnerabilidades do sistema com relação à possibilidade de violação de resultados e de quebra do sigilo do voto.

A quinta edição do TPS ocorreu entre 25 e 29 de novembro de 2019, no Edifício-Sede do TSE, em Brasília. O espaço foi preparado exclusivamente para o evento, com entrada controlada e ambiente monitorado por câmeras. Participaram do evento 22 investigadores, os quais tiveram acesso aos componentes internos e externos do sistema eletrônico de votação, para criarem seus planos de ataque.

Os participantes estavam divididos em cinco grupos e três eram investigadores individuais. Dos dez planos de teste apresentados, dois – realizados pelo Grupo 5, composto por investigadores da Polícia Federal – foram bem-sucedidos.

A primeira edição foi realizada de 10 a 13 de novembro de 2009. Durante os quatro dias, os participantes tentaram violar os sistemas, sem sucesso. Não foi detectada qualquer falha nas barreiras de proteção contra fraudes e tentativas de violação.

A segunda edição ocorreu entre 20 e 22 de março de 2012, quando foi detectada a necessidade de fortalecer a aleatoriedade da sequência dos votos a fim de evitar a identificação da ordem de registro dos votos, o que foi realizado imediatamente após a descoberta do problema. A não conformidade estava relacionada ao algoritmo de embaralhamento dos votos no Registro Digital do Voto (RDV), ou seja, à ordem de gravação dos votos de cada eleitor.

No total das duas edições (de 2009 e de 2012), foram executados 27 planos de ataques, com as mais engenhosas ideias, todas sem sucesso. Essas experiências foram, entretanto, extremamente positivas, pois deram ao TSE a chance de aperfeiçoar a segurança e aumentar a confiabilidade dos sistemas, a partir das análises e conclusões feitas pelos investigadores, o que incentivou a continuação da iniciativa em eleições posteriores.

Em 30 de abril de 2015, o Plenário aprovou a Resolução-TSE nº 23.444, que institucionalizou a realização periódica do TPS durante o ciclo de desenvolvimento dos sistemas de votação e de apuração, constituindo, obrigatoriamente, parte integrante do processo eleitoral brasileiro.

A terceira edição do TPS ocorreu durante os dias 8, 9 e 10 de março de 2016, no Edifício-Sede do TSE, em Brasília. Participaram do evento 13 investigadores, os quais tive-

ram acesso aos componentes internos e externos do sistema eletrônico de votação, para criarem seus planos de ataque.

A quarta edição foi realizada no período de 27 a 30 de novembro de 2017, com 14 participantes efetivos, sendo 3 grupos e 4 participantes individuais. Dos 13 planos de teste apresentados, 10 foram executados, dentre os quais 4 contribuíram para o aprimoramento do processo eleitoral e 6, não.

O TPS é uma ação decorrente da missão estratégica do TSE de "garantir a legitimidade do processo eleitoral e a efetiva prestação jurisdicional, a fim de fortalecer a democracia" e reúne investigadores independentes para, individualmente ou organizados em times, executarem planos de ataque aos componentes internos e externos da urna eletrônica.

2. O Teste Público de Segurança (TPS)

O TPS constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, de apuração, de transmissão e de recebimento de arquivos, e deve ser realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

Presidido pelo próprio presidente do TSE, o TPS é um evento aberto à participação da sociedade, com o objetivo de fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral, contemplando ações controladas a fim de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Os sistemas eleitorais que são objetos de investigação do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados.

2.1 Normas reguladoras

A Resolução-TSE nº 23.444/2015 (Anexo A) foi publicada com o objetivo de instituir a realização periódica do TPS no ciclo de desenvolvimento dos sistemas de votação e de apuração e permanece como principal norma sobre o tema, definindo-o como parte integrante do processo eleitoral brasileiro, devendo ser realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais. A resolução também indica a elaboração de edital específico para a realização das edições do teste.

Em 16 de agosto de 2019, foi publicado o edital do TPS 2019 (Anexo A), contemplando as regras específicas e as datas para a realização de todas as demais fases e ações. O edital foi debatido com a sociedade e as contribuições dos cidadãos foram incorporadas no texto final do edital.

2.2 Comissões

A Resolução-TSE nº 23.444/2015 definiu a atuação e as atribuições de quatro comissões: Comissão Organizadora, Comissão Reguladora, Comissão Avaliadora e Comissão de Comunicação Institucional, cujas composições estão no Anexo B.

Destaca-se, dentre elas, a Comissão Avaliadora, cuja composição se dá por: um representante indicado pelo ministro presidente do TSE; membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação; um representante do Ministério Público Federal (MPF); um representante da Ordem dos Advogados do Brasil (OAB); um representante do Congresso Nacional; um perito criminal federal da área de Informática, do Departamento de Polícia Federal; um engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (Crea), indicado pelo Conselho Federal de Engenharia e Agronomia (Confea); e um representante da Sociedade Brasileira de Computação (SBC). Essa comissão pode, ainda, valer-se de integrantes do TSE para assessorá-la.

A principal função dessa comissão foi avaliar e homologar os resultados obtidos no evento e produzir um relatório final conclusivo (Anexo H). Nesse relatório, foram registradas as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às possíveis fraudes identificadas durante o TPS.

2.3 Participação

Puderam participar do TPS 2019, na condição de técnico(s) e/ou de grupo(s) de técnicos, cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, que preenchessem os requisitos definidos no edital (Anexo A), que limitou a quantidade máxima de participantes a 25 pessoas, somando-se as participações individuais e em grupo, podendo cada equipe conter de dois a cinco membros. Também foi estabelecido o limite de 10 inscrições possíveis, isto é, a soma do número de grupos de investigadores e de investigadores individuais não poderia ultrapassar 10.

Foi vedada a participação de membros das comissões e de pessoas com mais de uma inscrição, seja em grupo ou individual.

2.4 Etapas

O TPS foi dividido – seguindo o definido no art. 17 da Resolução-TSE nº 23.444/2015 – nas fases de preparação, realização e avaliação.

a. Preparação

A fase de preparação consistiu no período em que os investigadores e/ou os grupos de investigadores puderam aprender sobre o funcionamento dos sistemas alvo de ataque no TPS. Ainda nesta fase, ocorreu a publicação do edital com as regras específicas e datas para a realização de todas as demais fases e ações do evento. Nesta última edição, foram elaborados vídeos explicativos sobre o processo eleitoral.

Foi disponibilizado local para a visualização do código-fonte. O acesso ao código só pôde ser realizado mediante assinatura de um termo de confidencialidade pelos grupos e pelos investigadores individuais, tendo sido vedada a extração, impressão e/ou reprodução, mesmo que parcial, do código-fonte e vedado o ingresso no ambiente segregado ao da realização dos testes com qualquer instrumento que permitisse a cópia do código-fonte. Foram permitidas apenas anotações que não confrontassem o termo de confidencialidade.

Nesta fase, também foram preparados e configurados os sistemas adicionais que foram utilizados no teste.

A solicitação para participação no evento foi dividida em duas etapas. Na primeira, o candidato preencheu o formulário de pré-inscrição e o enviou ao TSE. Na segunda, a inscrição foi realizada por meio do preenchimento de Plano de Teste, documento com o detalhamento de como se daria a tentativa de violação do sistema eletrônico de votação. O plano enviado pelos investigadores e pelos grupos de investigadores que tiveram a pré-inscrição aprovada foram submetidos à Comissão Reguladora, para avaliação.

b. Realização

Na fase de realização, os técnicos com inscrições homologadas compareceram ao TSE e realizaram os planos de teste previamente definidos, seguindo as regras do edital.

Ao final da realização do TPS, cada investigador ou grupo de investigadores apresentou relatório das ações executadas e dos resultados alcançados.

Os investigadores ou os grupos que identificassem alguma falha, vulnerabilidade explorada ou fraude no sistema eletrônico de votação deveriam, ao final, fazer sugestões de melhoria relacionadas aos erros encontrados.

c. Avaliação

Nesta fase, a Comissão Avaliadora elaborou relatório (Anexo H) contendo ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas.

3. Seleção de projetos

Para que suas inscrições fossem aprovadas, os investigadores precisaram apresentar planos de teste que seguissem as seguintes exigências, estipuladas no parágrafo único do art. 20 do edital do TPS 2019:

I. atenderem aos objetivos específicos de alterar a destinação dos votos ou fragilizar o sigilo do voto;

II. atenderem ao objeto estabelecido no edital[1];

[1] Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados;

III. demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou

IV. serem entregues no prazo estipulado no Marco 7 do calendário do evento (anexado ao final do edital do TPS, Anexo A).

O documento com a declaração dos inscritos aprovados e a avaliação dos planos de teste encontram-se nos Anexos D e E deste compêndio.

3.1 Projetos avaliados

Após a avaliação dos planos de teste, cinco grupos de investigadores e três investigadores individuais foram classificados para participar do TPS 2019. Treze planos foram aprovados, tendo sido executados efetivamente dez planos de teste.

Durante o evento, o grupo liderado por Paulo César Herrmann Wanner contou também com a participação de Ivo Peixinho e Galileu Batista de Souza, todos peritos da Polícia Federal. Apresentaram três planos de teste, sendo que dois deles foram bem-sucedidos: o de "extração do conteúdo do disco criptografado do SIS" e o de "instalação e execução de código arbitrário em uma máquina do Gedai para implante de dados falsos na urna eletrônica".

No Anexo E, estão todos os planos de teste submetidos à Comissão Reguladora, dentre os quais, os aprovados e os reprovados durante o processo de avaliação, assim como aqueles submetidos durante a realização dos testes. A seguir, estão apenas os planos aprovados durante a fase de seleção.

Investigadores/Grupos de investigadores aprovados	Resumo do plano de teste
Grupo 1	O teste proposto refere-se à identificação do eleitor e de seu voto a partir das informações gravadas no Registro Digital do Voto (RDV) e à tentativa de manipulação do Boletim de Urna (BU).
Grupo 2	Identificação da operação eletrônica da urna, analisando os sinais elétricos nos circuitos entre o teclado e a placa mãe e empregando técnicas de inteligência artificial para identificação de cada tecla pressionada.
Grupo 3	Propôs a realização de dois testes: 1) obtenção de chaves criptográficas e verificação do correto uso da criptografia para a garantia da integridade, confidencialidade e autenticidade; 2) verificação da proteção de programas pré-construídos (denominados de bibliotecas), necessários ao sistema da urna.
Grupo 4	Tentativa de uso de Machine Learning para reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

[2] Plano de teste submetido durante o evento e aceito pela Comissão Reguladora.

(Continuação)

Investigadores/Grupos de investigadores aprovados	Resumo do plano de teste
Grupo 5	Propôs realização de três testes: 1) recuperação de senhas de acesso dos sistemas de transmissão do BU para enviar votos falsos; 2) quebra da criptografia da proteção (SIS) do sistema gerador de mídia das urnas eletrônicas (Gedai); 3) domínio do sistema de geração de mídia a fim de adulterar dados de preparação da urna da seção eleitoral.
Investigador individual: **José Filippe de Moraes Albano**	Identificação de componentes da rede computacional do TSE, de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede.
Investigador individual: **Leonardo Cunha dos Santos**	Quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas.

4. Resultados

Os testes ocorreram entre 25 e 29 de novembro de 2019 e, após o término do evento, os membros da Comissão Avaliadora, de posse dos planos de teste e da documentação de execução dos testes (Anexo E), reuniram-se para elaboração do relatório de avaliação dos testes (Anexo H).

Em 29 de novembro de 2019, foi realizada no TSE divulgação preliminar dos resultados e das conclusões do TPS.

4.1 Conclusões/Soluções a serem tomadas

Diante dos registros de falhas identificadas durante os testes e apresentadas no relatório da Comissão Avaliadora, o TSE convocará os investigadores para executarem novamente os mesmos testes, em uma nova versão do sistema eleitoral, em que terão sido feitas as devidas correções. Essa nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano de teste que identificou a falha, vulnerabilidade explorada ou fraude. O plano pode ser alterado somente em função das correções realizadas nos sistemas afetados.

4.2 Encerramento e certificação

Em 29 de novembro de 2019, durante a divulgação preliminar dos resultados e das conclusões do TPS, foram entregues certificados de participação aos investigadores e aos grupos de investigadores.

Segue abaixo lista de investigadores ou de grupo de investigadores que obtiveram a certificação:

Grupo 1 – Fellipe Ribeiro Silva Abib (coordenador)

Grupo 2 – Jairo Simão Santana Melo (coordenador)

Grupo 3 – Luis Antonio Brasil Kowada (coordenador)

Grupo 4 – Luís Fernando de Almeida (coordenador)

Grupo 5 – Paulo César Herrmann Wanner (coordenador)

Investigador individual – José Filippe de Moraes Albano

Investigador individual – Leonardo Cunha dos Santos

Anexos

Anexo A – Normas para o Teste Público de Segurança 2019

Resolução nº 23.444/2015

Resolução nº 23.444, de 30 de abril de 2015 – Brasília – DF

Dispõe sobre a realização periódica do Teste Público de Segurança – TPS nos sistemas eleitorais que especifica.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das atribuições que lhe conferem o art. 23, IX, do Código Eleitoral e o art. 105 da Lei nº 9.504, de 30 de setembro de 1997, resolve expedir a seguinte instrução:

CAPÍTULO I

DO OBJETO

Art. 1º Fica instituído o Teste Público de Segurança TPS no ciclo de desenvolvimento dos sistemas de votação e apuração.

§ 1º O TPS de que trata esta resolução constitui parte integrante do processo eleitoral brasileiro e será realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

§ 2º A presidência dos trabalhos relativos ao TPS será exercida pelo Presidente do Tribunal Superior Eleitoral.

Art. 2º Os sistemas eleitorais que poderão ser objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, conforme definido no § 2º do art. 66 da Lei nº 9.504/1997, incluindo o *hardware* da urna e seus *softwares* embarcados.

CAPÍTULO II

DO OBJETIVO

Art. 3º O Teste Público de Segurança tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral.

Parágrafo único. O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

CAPÍTULO III

DAS DEFINIÇÕES

Art. 4º Para os fins desta resolução, considera-se:

I – Falha: evento em que se observa que um sistema violou sua especificação por ter entrado em um estado inconsistente ocasionado por uma imperfeição (defeito) em um *software* ou *hardware* impedindo seu bom funcionamento, sem interferir na destinação e/ou anonimato dos votos dos eleitores.

II – Vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas não seja condição suficiente para alcançar um dos objetivos definidos no parágrafo único do art. 3º.

III – Fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis.

IV – Plano de testes: documento que será fornecido para identificação e descrição das ações a serem desempenhadas pelo(s) técnico(s) e/ou grupo(s) de técnicos quando da realização do teste.

V – Ambiente de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para que o(s) técnico(s) e/ou o(s) grupo(s) de técnicos possam preparar e realizar os testes.

CAPÍTULO IV

DAS ATRIBUIÇÕES

Art. 5º As unidades do Tribunal Superior Eleitoral deverão atuar, observadas as respectivas atribuições, para a plena realização do teste instituído por esta resolução.

Art. 6º Atuarão no Teste Público de Segurança:

I – Comissão Organizadora;

II – Comissão Reguladora;

III – Comissão Avaliadora;

IV – Comissão de Comunicação Institucional.

Art. 7º A gerência geral da realização do TPS será feita por integrantes da Diretoria-Geral, designados por portaria do Presidente do Tribunal.

Art. 8º A Comissão Organizadora terá as seguintes atribuições:

I – planejar e elaborar o projeto geral para a realização do evento;

II – organizar e prover a infraestrutura necessária para a realização de todas as fases do TPS;

III – convocar as demais áreas do Tribunal, observadas as respectivas atribuições administrativas, a fim de providenciar ações ou infraestrutura para a realização do evento;

IV – manter informadas a Presidência e a Diretoria-Geral sobre o andamento dos trabalhos.

Parágrafo único. A Comissão Organizadora será composta pelas áreas da Diretoria-Geral, Administração, Segurança, Imprensa e Comunicação Social, Infraestrutura de TI e do Cerimonial.

Art. 9º A Comissão Reguladora terá as seguintes atribuições:

I – definir os procedimentos e a metodologia utilizados;

II – aprovar a(s) inscrição(ões) do(s) técnico(s) e/ou do(s) grupo(s) de técnicos que tenha(m) atendido às exigências constantes do edital;

III – supervisionar e documentar todas as fases do evento;

IV – aprovar os planos de testes elaborados pelo(s) técnico(s) e/ou grupo(s) de técnicos;

V – realizar outras atividades relacionadas à disciplina do TPS, visando ao fiel cumprimento do objetivo desta resolução, ressalvadas as atribuições das demais comissões e da Presidência do Tribunal Superior Eleitoral;

VI – elaborar, em conjunto com a Comissão Organizadora, a minuta do edital que disciplinará a convocação e as etapas do TPS.

Parágrafo único. Os componentes da Comissão de que trata o *caput* deste artigo serão indicados por portaria, entre os quais no mínimo um com conhecimentos jurídicos indicado pela Presidência do Tribunal, integrantes da Secretaria de Tecnologia da Informação e um integrante da Comissão de Comunicação Institucional, definida no art. 11 desta resolução.

Art. 10. A Comissão Avaliadora terá as seguintes atribuições:

I – validar a metodologia e os critérios de julgamento definidos pela Comissão Disciplinadora do Teste Público de Segurança;

II – avaliar e homologar os resultados obtidos e produzir relatório final conclusivo.

§ 1º A Comissão de que trata o *caput* deste artigo será nomeada pelo Presidente do Tribunal, com a seguinte composição:

I – um representante indicado pelo Ministro Presidente;

II – membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação;

III – um representante do Ministério Público Federal;

IV – um representante da Ordem dos Advogados do Brasil;

V – um representante do Congresso Nacional;

VI – um perito criminal federal da área de Informática, do Departamento de Polícia Federal;

VII – um engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (CREA), indicado pelo Conselho Federal de Engenharia e Agronomia (CONFEA);

VIII – um representante da Sociedade Brasileira de Computação (SBC).

§ 2º A Comissão poderá se valer de integrantes do Tribunal para assessorá-los.

§ 3º O Tribunal disponibilizará serviços de secretariado, espaço e infraestrutura à Comissão.

§ 4º Para a indicação dos integrantes definidos nos incisos III a VIII do § 1º deste artigo as respectivas instituições serão oficiadas para indicarem os componentes mencionados.

Art. 11. A Comissão de Comunicação Institucional terá as seguintes atribuições:

I – elaborar o plano de comunicação sobre o evento;

II – receber as solicitações de informação do público externo e centralizar a publicação de informações e notícias sobre o TPS, observadas as orientações da Presidência e da Diretoria-Geral;

III – responsabilizar-se pela cobertura jornalística do evento e credenciamento dos veículos de comunicação.

Parágrafo único. A Comissão de Comunicação Institucional será composta pelas áreas da Diretoria-Geral, Imprensa e Comunicação Social e Tecnologia da Informação.

CAPÍTULO V

DA PARTICIPAÇÃO

Art. 12. Poderão participar, na condição de técnico(s) e/ou de grupo(s) de técnicos, cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, que preencham os requisitos definidos em edital.

§ 1º O edital de que trata o *caput* disciplinará a quantidade máxima de participantes e equipes, bem como os critérios para inscrição, seleção e avaliação.

§ 2º Em caso de inscrições em quantidade superior à definida no edital de que trata o § 1º deste artigo, haverá sorteio público, entre as inscrições aprovadas.

Art. 13. É vedada a participação, na condição de técnico(s) e/ou grupo(s) de técnicos, de componentes das Comissões referidas no art. 6º desta resolução.

Art. 14. Para promover a participação no TPS, o(s) técnico(s) e/ou grupo(s) de técnicos que reside(m) fora do município de realização do evento poderá(ão) requerer passagens e diárias ao Tribunal Superior Eleitoral.

Parágrafo único. As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral, além daquelas estipuladas no respectivo edital.

Art. 15. Ao final da fase de realização do Teste Público de Segurança, cada técnico ou grupo de técnicos deverá apresentar Relatório Técnico das ações executadas e resultados alcançados, de acordo com as regras definidas em edital.

Art. 16. O(s) técnico(s) e/ou grupo(s) de técnicos, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, deverá(ão) apresentar a(s) respectiva(s) sugestão(ões) de melhoria.

§ 1º Em um prazo de até 6 (seis) meses após a realização do TPS, o(s) técnico(s) e/ou grupo(s) de técnicos poderá(ão) ser convocado(s) a executar novamente, em uma nova versão do sistema eleitoral com as devidas correções, os mesmos testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 2º A nova execução dos testes de que trata o parágrafo anterior não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas no sistema.

§ 3º Para o disposto no § 1º, as modificações realizadas serão apresentadas, observado o disposto no § 2º do artigo 18.

CAPÍTULO VI

DAS FASES DO TESTE PÚBLICO DE SEGURANÇA

Art. 17. O Teste Público de Segurança será dividido nas fases de preparação, realização e avaliação.

Art. 18. Na fase de preparação, deverão ser realizadas as seguintes ações ou eventos:

I – audiência pública com o objetivo de esclarecer as regras do TPS definidas nesta resolução;

II – publicação do edital que deverá contemplar as regras específicas e datas para a realização de todas as demais fases e ações do evento;

III – palestra informativa sobre o sistema eletrônico de votação com o objetivo de subsidiar os eventuais participantes sobre o funcionamento do sistema eleitoral;

IV – apresentação, em ambiente controlado, dos códigos-fonte dos sistemas eleitorais que farão parte do TPS;

V – geração de versão a ser utilizada no TPS, observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas;

VI – preparação e configuração dos sistemas adicionais que serão utilizados no teste e elaboração dos respectivos planos de teste;

VII – recebimento das inscrições e planos de teste dos técnicos que desejam participar do evento.

§ 1º Poderão ser definidas outras ações ou eventos intermediários para atender objetivos complementares desta fase, desde que estejam definidos no edital da respectiva edição do TPS.

§ 2º A apresentação dos códigos-fonte, de que trata o inciso IV deste artigo, será feita em ambiente controlado, com acesso mediante Termo de Confidencialidade e regras específicas definidas em edital.

Art. 19. Na fase de realização, os técnicos com inscrições homologadas comparecerão no local determinado para a realização do Teste Público de Segurança para executar no ambiente de teste os planos de teste previamente definidos, conforme regras definidas no edital.

Art. 20. Na fase de avaliação, a Comissão Avaliadora definida no art. 10, de posse dos planos de testes e documentação de execução dos testes, deverá elaborar relatório de avaliação contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas durante o TPS.

§ 1º O Tribunal promoverá evento de encerramento para demonstrar os resultados alcançados, que deverá contar com a presença do(s) técnico(s) e/ou grupo(s) de técnicos e Comissão Avaliadora.

§ 2º A Secretaria de Gestão da Informação será responsável por editar publicação específica, em formato físico e eletrônico, contendo um compêndio da documentação produzida e conclusões da Comissão Avaliadora.

§ 3º A publicação, em formato eletrônico, de que trata o parágrafo anterior deverá ser disponibilizada no sítio do Tribunal Superior Eleitoral.

CAPÍTULO VII

DAS DISPOSIÇÕES GERAIS

Art. 21. O edital que disciplinará cada edição do Teste Público de Segurança será publicado no *DJe*/TSE e divulgado no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 22. Será dada publicidade à composição das comissões descritas no art. 6º desta resolução no *DJ*e/TSE e no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 23. Os participantes do TPS que tiverem a inscrição aprovada deverão manter conduta ética nas declarações e ilações sobre as hipóteses e resultados encontrados.

Art. 24. Fica autorizada a contratação e/ou celebração de convênio com instituições renomadas para realizar a pré-avaliação da segurança dos sistemas eleitorais e assessorar a realização do TPS.

Art. 25. O Tribunal Superior Eleitoral promoverá a criação de uma unidade ou núcleo permanente para tratar sistematicamente as questões relativas à segurança do processo eleitoral informatizado e à realização do teste de que cuida esta norma.

Art. 26. Os casos omissos serão dirimidos pela Presidência do Tribunal Superior Eleitoral.

Art. 27. Esta Resolução entra em vigor na data de sua publicação.

Brasília, 30 de abril de 2015.

Ministro DIAS TOFFOLI, presidente e relator – Ministro GILMAR MENDES – Ministro LUIZ FUX – Ministro JOÃO OTÁVIO DE NORONHA – Ministra MARIA THEREZA DE ASSIS MOURA – Ministro HENRIQUE NEVES DA SILVA – Ministro ADMAR GONZAGA.

Publicada no *DJE* de 21.5.2015.

TRIBUNAL SUPERIOR ELEITORAL

EDITAL DO TESTE PÚBLICO DE SEGURANÇA

A Comissão Reguladora comunica aos interessados que, conforme estabelecido na Resolução-TSE nº 23.444, de 30 de abril de 2015, será realizado o Teste Público de Segurança no sistema eletrônico de votação, no período de 25 a 29 de novembro de 2019, nos horários estabelecidos no art. 32 deste edital, na sede do Tribunal Superior Eleitoral (Setor de Administração Federal Sul – SAFS, Quadra 7, lotes 1/2, Brasília/DF).

CAPÍTULO I

DO OBJETO

Art. 1º Constitui objeto deste edital a realização do Teste Público de Segurança (TPS) no sistema eletrônico de votação que será utilizado nas eleições municipais de 2020.

Parágrafo único. O TPS de que trata este edital constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, apuração, transmissão e recebimento de arquivos.

Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados.

§ 1º Os componentes de *software* e *hardware* que serão objeto do TPS consistem em:

I - Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE);

II - *Software* Básico da Urna Eletrônica, *Software* de Carga (SCUE), Gerenciador de Aplicativos (GAP), *Software* de Votação (VOTA), Recuperador de Dados (RED) e Sistema de Apuração (SA);

III - Sistemas Transportador, RecArquivos e InfoArquivos;

IV - Subsistema de Instalação e Segurança (SIS) e Kit JE Connect;

V - Urna modelo 2015, com seus respectivos *firmwares* e mídias eletrônicas.

§ 2º Não serão objetos do TPS os seguintes sistemas, ambientes, procedimentos e elementos abaixo relacionados:

I - identificação e verificação biométrica do eleitor;

II - preparação e infraestrutura para o Kit JE Connect;

III - 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);

IV - totalização (TOT) e gerenciamento da totalização (GER);

V - acesso às máquinas servidoras;

VI - acesso aos bancos de dados;

VII - ataques de negação de serviço;

VIII - ataque destrutivo à urna eletrônica e demais recursos computacionais da Justiça Eleitoral;

IX - sistema de geração de chaves criptográficas;

X - alteração do código-fonte dos sistemas;

XI - ambiente de compilação dos sistemas;

XII - lacre físico: selos autoadesivos utilizados na urna eletrônica com a finalidade de detectar eventuais violações ao equipamento.

§ 3º Conforme o § 2º do art. 66 da Lei nº 9.504, de 30 de setembro de 1997, as chaves eletrônicas privadas e senhas eletrônicas de acesso manter-se-ão sob sigilo da Justiça Eleitoral.

§ 4º A versão dos sistemas a ser utilizada no TPS será gerada observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas, no que couber.

CAPÍTULO II

DO OBJETIVO

Art. 3º O TPS tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar aperfeiçoamento do processo eleitoral.

Parágrafo único. O TPS contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição e apresentar as respectivas sugestões de melhoria.

CAPÍTULO III

DAS DEFINIÇÕES

Art. 4º Para fins deste edital, considera-se:

I - falha: evento em que se observa que um sistema violou sua especificação por ter entrado em estado inconsistente ocasionado por uma imperfeição (defeito) em um *software* ou *hardware*, impedindo seu bom funcionamento, sem interferir na destinação e/ou anonimato dos votos dos eleitores;

II - vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas que não seja condição suficiente para violar a destinação ou sigilo dos votos, ou, caso sejam alcançados, que deixe a existência de vestígios;

III - fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis;

IV - plano de teste: documento que será fornecido para identificação e descrição das ações a serem desempenhadas pelos investigadores e/ou grupos de investigadores na ocasião da realização do teste;

V - ambiente de execução de plano de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para que os investigadores e/ou grupos de investigadores

possam preparar e realizar os testes;

VI - ambiente de apresentação dos códigos-fonte: área interna ao ambiente de execução de plano de teste preparado para que os investigadores possam avaliar os códigos-fonte;

VII - teste de confirmação: reprodução pelo investigador ou grupo de investigadores do teste realizado durante o TPS, no qual foi identificada falha, vulnerabilidade explorada ou fraude, em uma nova versão do sistema eleitoral, com as devidas correções, com o intuito de avaliar a melhoria implementada.

CAPÍTULO IV

DA COORDENAÇÃO E DA ATUAÇÃO NO TESTE PÚBLICO DE SEGURANÇA

Art. 5º O TPS será coordenado pelo Ministro Presidente do Tribunal Superior Eleitoral (TSE).

Art. 6º Conforme estabelecido no art. 6º da Resolução-TSE nº 23.444/2015, atuarão no TPS:

I - Comissão Organizadora;

II - Comissão Reguladora;

III - Comissão Avaliadora;

IV - Comissão de Comunicação Institucional; e

V - investigadores e/ou grupos de investigadores.

CAPÍTULO V

DA COMUNICAÇÃO E DOS PRAZOS

Art. 7º Todos os formulários e documentos a serem remetidos ao TSE para fins de pré-inscrição, inscrição, manifestação e recurso deverão ser:

I - encaminhados por SEDEX ou carta registrada endereçados à Secretaria de Tecnologia da Informação do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF, CEP 70070-600); ou

II - protocolizados no Protocolo Administrativo, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF); ou

III - encaminhados para o *e-mail* tps2019@tse.jus.br; ou

IV - quando disponíveis, pelo sítio oficial do TPS (justicaeleitoral.jus.br/tps).

§ 1º Por não dispor de comprovação de recebimento e leitura, a comunicação por intermédio de *e-mail* é meramente alternativa e tem o objetivo de facilitar a comunicação dos investigadores ou grupo de investigadores.

§ 2º O Tribunal confirmará o recebimento de *e-mail* imediatamente após proceder à leitura da mensagem.

§ 3º No caso de o investigador ou o grupo de investigadores não receber a confirmação de leitura ou de recebimento pelo TSE, no prazo por ele julgado conveniente, deverá encaminhar o conteúdo da mensagem e/ou material anexo por SEDEX ou protocolizá-lo no Tribunal, respeitando-se os prazos estabelecidos neste edital.

Art. 8º O sítio oficial do TPS será justicaeleitoral.jus.br/tps.

§ 1º As informações relacionadas ao evento serão publicadas no sítio oficial do TPS.

§ 2º Mensagens eletrônicas recebidas de investigadores ou grupo de investigadores serão respondidas por *e-mail*, exceto se a resposta for de interesse geral, quando poderá ser publicada no sítio oficial do TPS.

Art. 9º As datas e prazos que norteiam o TPS estão informados no Calendário do Evento, anexo a este edital.

§ 1º Os prazos poderão ser prorrogados a critério do TSE.

§ 2º Quaisquer alterações de datas serão informadas no sítio oficial do TPS.

CAPÍTULO VI

DA PARTICIPAÇÃO

Art. 10. O TPS terá no máximo 25 participantes, observando-se o seguinte:

I - a participação poderá ser individual (investigador) ou em grupo de investigadores;

II - cada grupo de investigadores poderá ter de 2 a 5 membros;

III - um participante não pode possuir mais de uma inscrição, seja em grupo ou individual; e

IV - o total de grupos de investigadores somado ao de investigadores individuais não poderá ser superior a 10, ou seja, serão aceitas até 10 inscrições.

Parágrafo único. É vedada a participação, na condição de investigador e/ou de grupo de investigadores, de componentes das comissões definidas no art. 6º da Resolução-TSE nº 23.444/2015.

Art. 11. A participação, na condição de investigador e/ou de grupo de investigadores, está condicionada à seleção prévia, que será realizada em 3 etapas:

I - aprovação da pré-inscrição;

II - aprovação da inscrição; e

III - disponibilidade orçamentária e sorteio público.

Parágrafo único. A Comissão Avaliadora poderá, a seu critério, selecionar os planos de testes de até 2 investigadores ou grupos de investigadores que não foram sorteados.

CAPÍTULO VII

DA PRÉ-INSCRIÇÃO

Art. 12. A pré-inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Pré-Inscrição, que poderá ser obtido no sítio oficial do TPS.

Art. 13. O formulário Pré-Inscrição preenchido e os documentos comprobatórios exigidos deverão ser encaminhados, postados ou protocolizados no TSE, respeitados os prazos estabelecidos no Marco 1 do Calendário do Evento.

Art. 14. Terão sua pré-inscrição aprovada, na condição de investigador ou de grupo de investigadores, os cidadãos brasileiros maiores de 18 anos que preencham os requisitos constantes do formulário de pré-inscrição.

§ 1º Cada grupo de investigadores deverá designar um de seus componentes para representá-lo.

§ 2º Das pré-inscrições deverão constar os dados referentes a todos os componentes do grupo.

§ 3º Caso um dos membros do grupo de investigadores não atenda aos

requisitos do formulário de pré-inscrição, o grupo não terá sua pré-inscrição aprovada.

§ 4º Os investigadores ou grupos de investigadores deverão informar, no momento do preenchimento do formulário de pré-inscrição, se desejam fazer uso de recursos financeiros do TSE para o custeio de diárias e passagens.

§ 5º Pessoa jurídica poderá pré-inscrever-se, observando-se que:

I - terá sua pré-inscrição aprovada a pessoa jurídica cujo investigador e/ou grupo de investigadores que a representará no TPS cumpra todas as exigências do edital;

II - não serão aceitas pré-inscrições de empresas sem registro no Cadastro Nacional de Pessoa Jurídica (CNPJ).

Art. 15. Na data estabelecida no Marco 2 do Calendário do Evento serão publicadas as pré-inscrições aprovadas no sítio oficial do TPS.

§ 1º O investigador ou grupo de investigadores que não tiver sua pré-inscrição aprovada poderá apresentar recurso ao Tribunal.

§ 2º O recurso deverá ser encaminhado, postado ou protocolizado no TSE, respeitado o prazo estabelecido no Marco 3 do Calendário do Evento.

§ 3º O resultado do recurso será apresentado no sítio oficial do TPS na data prevista no Marco 4 do Calendário do Evento.

Art. 16. A palestra de que trata a resolução será realizada por meio de vídeos explicativos conforme o Marco 5 do Calendário do Evento.

Art. 17. Os investigadores e/ou grupos de investigadores com a pré-inscrição aprovada poderão agendar, respeitado o prazo estabelecido no Marco 6 do Calendário do Evento, visita à Sede do TSE para inspeção dos códigos-fonte.

§ 1º Os investigadores terão acesso ao código por meio de ferramenta de visualização fornecida pelo TSE.

§ 2º Só terão acesso aos códigos-fonte os investigadores e/ou grupos de investigadores que assinarem o termo de responsabilidade.

§ 3º Deverão assinar o termo de responsabilidade todos os investigadores que ingressarem no ambiente de apresentação dos códigos-fonte, mesmo que sejam membros de grupo.

§ 4º A assinatura do termo de responsabilidade dar-se-á no momento de ingresso do investigador no ambiente de apresentação dos códigos-fonte.

§ 5º Serão publicados no sítio oficial do TPS:

I - o modelo do termo de responsabilidade para fins de conhecimento prévio dos investigadores e/ou grupos de investigadores; e

II - o período reservado para a inspeção dos códigos-fonte.

§ 6º O tempo destinado aos investigadores e/ou grupo(s) de investigadores para inspeção dos códigos-fonte será estabelecido pelo TSE conforme a capacidade do ambiente e a quantidade de investigadores que manifestarem interesse.

§ 7º A assinatura digital dos códigos-fonte a serem inspecionados será realizada no primeiro dia do período estabelecido no Marco 6, sendo facultada aos investigadores presentes desde que estejam de posse de certificado digital padrão ICP Brasil.

§ 8º Não haverá custeio pelo Tribunal de diárias e passagens para essa fase do evento.

CAPÍTULO VIII

DA INSCRIÇÃO

Art. 18. A inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Plano de Teste, que poderá ser obtido no sítio oficial do TPS.

§ 1º Poderão apresentar plano de teste todos os investigadores e/ou grupos de investigadores com pré-inscrição aprovada.

§ 2º Cada investigador e/ou grupo de investigadores poderá apresentar mais de um plano de teste.

Art. 19. O formulário Plano de Teste preenchido e os documentos complementares, caso haja, deverão ser encaminhados, postados ou protocolizados no TSE, respeitado o prazo estabelecido no Marco 7 do Calendário do Evento.

Art. 20. Terão sua inscrição aprovada, na condição de investigador e/ou de grupo de investigadores, aqueles que tiverem seu plano de teste aprovado pela Comissão Reguladora.

Parágrafo único. Não serão aprovados os planos de testes que:

I - não atenderem aos objetivos específicos de alterar a destinação dos

votos ou fragilizar o sigilo do voto;

II - não atenderem ao objeto estabelecido no art. 2º deste edital;

III - não demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou

IV - forem entregues após o prazo estipulado no Marco 7 do Calendário do Evento.

Art. 21. Na data estabelecida no Marco 8 do Calendário do Evento, serão publicadas as inscrições aprovadas no sítio oficial do TPS.

§ 1º Os investigadores e/ou grupos de investigadores que não tiveram sua inscrição aprovada poderão apresentar recurso ao Tribunal, respeitado o prazo estabelecido no Marco 9 do Calendário do Evento.

§ 2º O resultado do recurso será apresentado no sítio oficial do TPS na data prevista no Marco 10 do Calendário do Evento.

Art. 22. A aprovação da inscrição do investigador e/ou do grupo de investigadores não garante a participação nos testes públicos de segurança.

CAPÍTULO IX

DA DISPONIBILIDADE ORÇAMENTÁRIA E DO SORTEIO PÚBLICO

Art. 23. Caso a quantidade de investigadores e/ou grupos de investigadores com inscrição aprovada seja superior à quantidade estipulada no art. 10 deste edital, far-se-á necessário realizar uma seleção entre as inscrições aprovadas, que será realizada na seguinte sequência:

I - serão selecionados os investigadores individuais que não necessitem de recursos financeiros do TSE para o custeio de diárias e passagens e, verificada quantidade de investigadores individuais selecionados superior a 10, será realizado sorteio público entre eles e recusadas as demais inscrições aprovadas;

II - após a seleção dos investigadores individuais, caso haja disponibilidade de vagas, serão selecionados os grupos de investigadores que não necessitem de recursos financeiros do TSE para o custeio de diárias e passagens:

a) havendo grupos de investigadores que não necessitem do custeio de diárias e passagens em quantidade superior à quantidade de vagas, realizar-

se-á sorteio entre os grupos respeitando-se os limites estabelecidos neste edital; e

b) caso todas as vagas tenham sido preenchidas, serão recusadas as demais inscrições aprovadas;

III - havendo disponibilidade de vagas:

a) será verificada a disponibilidade orçamentária do TSE para o custeio de diárias e passagens;

b) será realizado um orçamento do custo de diárias e passagens por investigador individual ou grupo de investigadores;

c) serão priorizados os investigadores ou grupos de investigadores com menor custo de diárias e passagens até o limite de vagas.

Art. 24. O sorteio público será realizado nas instalações do TSE, em data estabelecida no Marco 11 do Calendário do Evento.

Art. 25. Na data estabelecida no Marco 12 do Calendário do Evento, será publicado o resultado das inscrições selecionadas no sítio oficial do TPS.

§ 1º O investigador e/ou grupo de investigadores que não teve sua inscrição selecionada poderá apresentar recurso ao Tribunal, respeitado o prazo estabelecido no Marco 13 do Calendário do Evento.

§ 2º O resultado do recurso será apresentado no sítio oficial do TPS, na data estabelecida no Marco 14 do Calendário do Evento.

CAPÍTULO X

DAS INSCRIÇÕES SELECIONADAS

Art. 26. Os investigadores ou grupos de investigadores que optaram pelo custeio de deslocamento pelo TSE e que tiveram sua inscrição selecionada deverão requerer passagens e diárias ao Tribunal.

§ 1º As passagens e diárias devem ser requeridas até a data estabelecida no Marco 15 do Calendário do Evento, utilizando-se do formulário Solicitação de Diárias e Passagens, disponível no sítio oficial do TPS.

§ 2º As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral.

§ 3º O custeio de diárias compreenderá o período equivalente às fases de realização do TPS (Resolução nº 23.444/2015, art. 14) e do Teste de

Confirmação (Resolução nº 23.444/2015, art. 16), conforme estabelecido nos Marcos 16 e 19 do Calendário do Evento.

§ 4º Será aferida a presença por meio de lista a ser assinada pelos participantes durante o evento.

§ 5º O Tribunal deverá requerer o reembolso do investigador ou membro do grupo de investigadores que:

I - tiver passagens e/ou diárias custeadas pelo Tribunal e não comparecer ao evento;

II - receber quantidade de diárias maior do que o período de comparecimento ao evento; e

III - outros casos em que a Comissão Reguladora entender que o plano de teste não foi executado conforme definido e por responsabilidade exclusiva do investigador ou grupo de investigadores.

Art. 27. Os investigadores ou grupos de investigadores selecionados declaram ter ciência de que:

I - devem disponibilizar à Comissão Reguladora toda a documentação sobre os materiais utilizados e seus procedimentos durante as atividades, independentemente do resultado obtido no TPS;

II - devem apresentar à Comissão Reguladora todos os materiais utilizados e seus procedimentos durante as atividades; e

III – autorizam o uso de sua imagem pela Justiça Eleitoral, com a finalidade de divulgar o processo do TPS realizado pelo TSE, entendendo-se como imagem qualquer forma de representação, inclusive a fotográfica, bem como o processo audiovisual que resulta da fixação de imagens, com ou sem som, que tenha a finalidade de criar, por meio de sua reprodução, a impressão de movimento, independentemente dos processos de sua captação, do suporte usado inicial ou posteriormente para fixá-lo e dos meios utilizados para sua veiculação.

Art. 28. Os investigadores e/ou grupos de investigadores com a inscrição selecionada e que tenham interesse, na data estabelecida no Marco 16 do Calendário do Evento, das 9 às 18 horas, na Sede do TSE, poderão inspecionar os códigos-fonte do sistema eletrônico de votação.

Parágrafo único. Só terão acesso aos códigos-fonte os investigadores e/ou grupos de investigadores que assinarem termo de responsabilidade.

I - deverão assinar o termo de responsabilidade todos os investigadores que ingressarem no ambiente de apresentação dos códigos-fonte, mesmo que sejam membros de grupo;

II - estarão dispensados de assinar o termo de responsabilidade os investigadores ou grupo de investigadores que já o tenham feito na fase de pré-inscrição;

III - a assinatura do termo de responsabilidade dar-se-á no momento de ingresso do investigador no ambiente de apresentação dos códigos-fonte.

CAPÍTULO XI

DO TESTE PÚBLICO DE SEGURANÇA

Art. 29. O Tribunal Superior Eleitoral disponibilizará aos investigadores e/ou grupos de investigadores, no ambiente do TPS, os seguintes materiais e equipamentos:

I - folhas de papel em branco;

II - canetas esferográficas;

III - mesas;

IV - cadeiras;

V - microcomputadores padrão IBM-PC com plataforma Windows e/ou Ubuntu Linux 64 bits, que não poderão ser conectados à Internet;

VI - impressoras;

VII - chave Philips; e

VIII - urna eletrônica modelo 2015.

Parágrafo único. Será de responsabilidade dos investigadores e/ou grupos de investigadores a configuração dos equipamentos necessários à realização de seu plano de testes de segurança.

Art. 30. O microcomputador disponibilizado pelo TSE (art. 29, V), a urna eletrônica (art. 29, VIII) e os demais equipamentos, eventualmente preparados pelos investigadores e/ou grupos de investigadores participantes, serão lacrados ao término da preparação.

§ 1º Os equipamentos referidos no *caput* deste artigo terão sua integridade verificada no dia do teste pelos investigadores e/ou grupo de investigadores e pelos componentes das comissões referidas no art. 6º deste

edital.

§ 2º Eventual alteração no plano de testes, já entregue pelos investigadores e/ou grupos de investigadores e aprovado pela Comissão Reguladora, ficará sujeita à nova aceitação.

Art. 31. Durante a realização do TPS, os códigos-fonte estarão disponíveis para consulta, no ambiente de apresentação dos códigos-fonte, observando-se as seguintes condições:

I - é vedada a extração, impressão e/ou reprodução, mesmo que parcial, do código-fonte;

II - é vedado ingressar no ambiente de apresentação dos códigos-fonte com qualquer instrumento que permita a cópia do código-fonte;

III - são permitidas anotações que não confrontem o termo de responsabilidade:

a) as anotações estarão sujeitas à análise da Comissão Reguladora;

b) compete ao investigador responsabilizar-se por suas anotações; e

c) as anotações serão de uso restrito ao ambiente do TPS.

Parágrafo único. As vedações referidas nos incisos I e II deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente de apresentação dos códigos-fonte.

Art. 32. O TPS no sistema eletrônico de votação realizar-se-á em período estabelecido no Marco 16 do Calendário do Evento, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF).

Parágrafo único. O evento se iniciará às 13 horas do primeiro dia do período estabelecido no Marco 16 e findará às 17 horas do último dia do período estabelecido no Marco 17; nos demais dias os testes realizar-se-ão das 9 às 18 horas.

Art. 33. Somente serão executados os planos de testes dos investigadores e/ou grupos de investigadores que:

I - tiverem sua inscrição aprovada e selecionada;

II - estiverem presentes no momento da realização dos testes.

§ 1º Somente serão autorizados os planos de testes que forem aprovados e atendam aos requisitos deste edital, que não causem danos físicos aos equipamentos e às instalações disponibilizados para os citados testes e que forem tecnicamente viáveis.

§ 2º Para fins do inciso II deste artigo, os grupos de investigadores poderão ser representados por apenas um de seus componentes, ressalvado os que receberam diárias e passagens custeadas pela Justiça Eleitoral.

Art. 34. Ao final da fase de realização do TPS, cada investigador ou grupo de investigadores deverá apresentar Relatório do Investigador das ações executadas e resultados alcançados, de acordo com as regras definidas neste edital.

Art. 35. Os investigadores e/ou grupos de investigadores, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, deverão apresentar as respectivas sugestões de melhoria.

§ 1º Em data estabelecida pelo TSE, anterior à Cerimônia Oficial de Assinatura Digital e Lacração dos Sistemas a serem utilizados nas eleições de 2020, os investigadores e/ou grupos de investigadores poderão ser convocados a repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 2º A nova execução dos testes de que trata o § 1º deste artigo não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.

§ 3º Para o disposto no § 1º deste artigo, as modificações realizadas serão apresentadas de acordo com o cronograma a ser definido pela Comissão Reguladora.

§ 4º Os investigadores e/ou grupos de investigadores somente poderão manifestar-se publicamente sobre a falha ou vulnerabilidade encontrada após a divulgação do relatório da Comissão Avaliadora.

CAPÍTULO XII

DA DIVULGAÇÃO DOS RESULTADOS

Art. 36. Em data estabelecida no Marco 18 do Calendário do Evento, após o encerramento dos trabalhos, na Sede do TSE, será realizada uma divulgação preliminar dos resultados obtidos com o TPS e entregue o certificado de participação aos investigadores e grupos de investigadores.

§ 1º Será concedido o certificado aos investigadores e grupos de

investigadores que tiveram seus planos de testes devidamente executados, independentemente do resultado.

§ 2º Além do disposto no § 1º deste artigo, somente será concedido o certificado aos componentes dos grupos que estiveram presentes na ocasião da realização do respectivo teste de segurança.

§ 3º O local será divulgado no sítio oficial do TPS.

Art. 37. Em data estabelecida no Marco 19 do Calendário do Evento, das 10 às 11 horas, na Sede do TSE, será realizada a divulgação final dos resultados e das conclusões do TPS.

Parágrafo único. O local será divulgado no sítio oficial do TPS.

CAPÍTULO XIII

DO TESTE DE CONFIRMAÇÃO

Art. 38. Em data estabelecida no Marco 20 do Calendário do Evento, os investigadores e/ou grupos de investigadores serão convocados a repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 1º Durante o Teste de Confirmação, será disponibilizada visualização do código-fonte no ambiente de apresentação dos códigos-fonte, conforme o art. 33 deste edital.

§ 2º A nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.

§ 3º As modificações realizadas serão apresentadas no período de realização do Teste de Confirmação, conforme o Marco 20, estabelecido no calendário de eventos.

§ 4º Os grupos de investigadores poderão ser representados por apenas um de seus componentes, ressalvado os que receberam diárias e passagens custeadas pela Justiça Eleitoral.

CAPÍTULO XIV

DAS DISPOSIÇÕES GERAIS

Art. 39. As atividades executadas durante a inspeção dos códigos, a realização do TPS e o teste de confirmação poderão ser registradas pelo TSE em áudio e vídeo.

Art. 40. Para ingresso no ambiente destinado à realização do TPS, deverá ser observado que:

I - o ingresso com CD-ROM ou DVD-ROM, já utilizado e desde que não regravável, será autorizado; mídias virgens de CD-R ou DVD-R deverão ser identificadas e entregues à Comissão Reguladora antes de ingressar no ambiente destinado à realização do Teste Público de Segurança com o fim exclusivo de atendimento ao disposto no Art. 42 incisos II e III;

II - a entrada de outros equipamentos ou dispositivos além daqueles citados no inciso I deste artigo, desde que não tenham acesso à Internet, deverá ser autorizada pela Comissão Reguladora;

III - os investigadores e/ou grupos de investigadores poderão utilizar os *softwares* que julgarem necessários e instalá-los no microcomputador disponibilizado pelo TSE, observando-se o disposto nos incisos I e II deste artigo;

IV - o ingresso com materiais impressos será permitido;

V - os equipamentos, dispositivos eletrônicos e materiais citados nos incisos I, II e III deste artigo, quando aprovados, poderão ficar retidos no TSE por até 60 dias após o encerramento da realização do TPS.

§ 1º Os equipamentos ou dispositivos que tenham ficado retidos no TSE estarão à disposição dos participantes após o prazo citado no inciso V deste artigo.

§ 2º As vedações referidas nos incisos I a V deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente destinado à realização do TPS.

Art. 41. O ingresso no ambiente do TPS e no ambiente de apresentação dos códigos-fonte será restrito:

I - aos investigadores e/ou grupos de investigadores;

II - aos integrantes das comissões referidas no art. 6º deste edital;

III - às demais pessoas autorizadas pela Comissão Reguladora.

Art. 42. Haverá, no ambiente do TPS, computadores conectados à Internet para eventuais consultas pelos investigadores e/ou grupos de investigadores, sob supervisão da Comissão Reguladora.

I – os computadores referidos no *caput* deste artigo terão acesso a um drive de rede disponibilizado pela Comissão Organizadora, onde poderão ser salvos arquivos com conteúdo baixado da Internet;

II – os investigadores e/ou grupos de investigadores que salvarem arquivos no drive de rede referido no inciso I deste artigo deverão informar à Comissão Organizadora, solicitando que os mesmos sejam gravados em mídia CD-R ou DVD-R de sua propriedade, previamente entregues à Comissão Organizadora, conforme disposto no Art. 40 inciso I;

III – as mídias gravadas conforme disposto no inciso II deste artigo serão imediatamente entregues aos respectivos investigadores e/ou grupo de investigadores;

IV – eventuais mídias de CD-R ou DVR-R virgens não utilizadas somente serão devolvidas aos investigadores e/ou grupos de investigadores quando estes deixarem o ambiente destinado à realização do Teste Público de Segurança;

V – os computadores referidos no *caput* deste artigo terão acesso a uma impressora conectada em rede para eventuais impressões de documentos baixados da Internet, não sendo permitido:

a) a impressão de qualquer outro conteúdo,

b) a edição do conteúdo baixado antes da respectiva impressão, e

c) deixar o ambiente destinado à realização do Teste Público de Segurança portando qualquer uma destas folhas impressas;

VI – as folhas impressas através do disposto no inciso V deste artigo deverão ser solicitadas à Comissão Reguladora que, após verificar sua conformidade com as limitações definidas nas alíneas ‘a’ e ‘b’ do inciso V deste artigo, as disponibilizará imediatamente.

Art. 43. A Comissão Avaliadora somente poderá ter acesso ao código-fonte em caso de necessidade inafastável, sendo o acesso autorizado pela Comissão Reguladora, mediante a assinatura de termo de responsabilidade.

Art. 44. Este edital será publicado no *DJe*/TSE e divulgado no sítio eletrônico do Tribunal.

Art. 45. Será dada publicidade à composição das comissões referida art. 6º deste edital por meio do *DJe*/TSE e de divulgação no sítio oficial do T

Art. 46. Integra este edital o cronograma do TPS, em anexo.

Art. 47. Os casos omissos serão dirimidos pelo Presidente do TSE, poderá delegar a atribuição a Ministro ou a servidor do Tribunal.

Brasília, 16 de agosto de 2019.

ANEXO – CALENDÁRIO DO EVENTO

Marco	Referência	Descrição do marco	Prazo/período
1	Art. 13	Encaminhamento do formulário de Pré-Inscrição preenchido e dos documentos comprobatórios exigidos.	16/8 a 29/9/2019
2	Art. 15	Publicação das pré-inscrições aprovadas.	03/10/2019
3	§ 2º do art. 15	Apresentação de recurso referente à fase de pré-inscrição.	04 a 08/10/2019
4	§ 3º do art. 15	Publicação do resultado do recurso referente à fase de pré-inscrição.	10/10/2019
5	Art. 16	Disponibilização de vídeos explicativos sobre o processo eleitoral.	14/10/2019
6	Art. 17	Assinatura e inspeção dos códigos-fonte.	14 a 18/10/2019
7	Art. 19	Encaminhamento do formulário Plano de Teste preenchido e dos documentos complementares, caso haja.	14 a 27/10/2019
8	Art. 21	Publicação das inscrições aprovadas.	30/10/2019
9	§ 1º do art. 21	Apresentação de recursos referentes à fase de inscrição aprovada.	31 a 03/11/2019
10	§ 2º do art. 21	Publicação do resultado do recurso referente à fase de inscrição aprovada.	05/11/2019
11	Art. 24	Sorteio público para seleção de inscrições.	06/11/2019
12	Art. 25	Publicação do resultado das inscrições selecionadas.	06/11/2019
13	§ 1º do art. 25	Apresentação de recursos referentes à fase de inscrição selecionada.	07 a 10/11/2019
14	§ 2º do art. 25	Publicação do resultado do recurso referente à fase de inscrição selecionada.	11/11/2019
15	§ 1º do art. 26	Requisição de passagens e diárias.	12 a 20/11/2019
16	Art. 32	Abertura dos testes públicos de segurança e credenciamento dos investigadores.	25/11/2019
17	Art. 32	Realização dos testes públicos de segurança.	25 a 29/11/2019
18	Art. 36	Divulgação preliminar dos resultados do Teste Público de Segurança e entrega do certificado de participação.	29/11/2019
19	Art. 37	Divulgação do resultado final do Teste Público de Segurança.	10/12/2019
20	Art. 38	Realização do Teste de Confirmação	27/04/2020 a 29/04/2020

Anexo B – Portarias de designação das comissões

Portaria nº 483 de 24 de junho de 2019

Institui as Comissões Organizadora, Reguladora e de Comunicação Institucional, referentes ao Teste Público de Segurança 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto nos arts. 8°, 9° e 11 da Resolução-TSE n° 23.444, de 30 de abril de 2015,

RESOLVE:

Art. 1º Ficam instituídas as Comissões Organizadora, Reguladora e de Comunicação Institucional, que atuarão no Teste Público de Segurança 2019, nos termos previstos na Resolução-TSE n° 23.444, de 30 de abril de 2015, com a seguinte composição:

I - COMISSÃO ORGANIZADORA:

a) Thiago Fini Kanashiro (Agel/DG), representante da Secretaria do Tribunal, como coordenador dos trabalhos;

b) Cristiane Vale de Sousa (Cenaq/SAD), representante da Secretaria de Administração;

c) Antônio César da Silva Medeiros (COSGI/SST), representante da Secretaria de Segurança e Transporte;

d) Ana Cristina Rosa (Ascom/SPR), representante da Assessoria de Comunicação;

e) Luciano Teixeira Andrade (Seau/Coinf/STI), representante da Secretaria de Tecnologia da Informação;

f) Paula Cristiane Amorim de Souza (ACP/SPR), representante da Assessoria de Cerimonial; e

g) Marlon Van Juen Sun (Seeve/Coede/SGP), representante da Secretaria de Gestão de Pessoas.

II - COMISSÃO REGULADORA:

a) Giuseppe Dutra Janino (STI), representante da Secretaria de Tecnologia da Informação, como coordenador dos trabalhos;

b) Ana Paula Vilela de Pádua (Gab. Presidência), representante da Presidência.

c) Thiago Fini Kanashiro (Agel/DG), representante da Secretaria do Tribunal;

d) Rakell Cabral Dimanski (Ascom/SPR), representante da Comissão de Comunicação Institucional;

e) Elmano Amâncio de Sá Alves(Asag/STI);

f) Cristiano Moreira Andrade (Coinf/STI);

g) Rafael Fernandes de Barros Costa Azevedo (Cotel/STI);

h) José de Melo Cruz (Csele/STI);

i) Rodrigo Carneiro Munhoz Coimbra (Sevin/Csele/STI);

j) Júlio Valente da Costa Júnior (Setot/Csele/STI);

k) Célio Castro Wermelinger (Sipt/Cotel/STI);

l) Marcelo Carneiro Rodrigues (Sesop/Coinf/STI);

m) Ivanildo Ferreira Gomes (Sesap/Coinf/STI);

n) Alberto Araújo Cavalcante Neto (Seint/Csele/STI);

o) Cristiano Peçanha Corrêa (Sescon/Cogti/STI);

p) Carlos Eduardo Miranda Zottmann (Cogti/STI); e

q) Luís Augusto Consularo (Segele/Cotel/STI).

r) Antônio Ésio Marcondes Salgado (colaborador). (Redação dada pela Portaria nº 893/2019)

III - COMISSÃO DE COMUNICAÇÃO INSTITUCIONAL:

a) Ana Cristina Rosa (Ascom/SPR), representante da Assessoria de Comunicação, como coordenadora dos trabalhos;

b) Giuseppe Dutra Janino (STI), representante da Secretaria de Tecnologia da Informação.

c) Thiago Fini Kanashiro (Agel/DG), representante da Secretaria do Tribunal;

d) Nerinês Soares Accioly (Ascom/SPR);

e) Ana Paula da Rosa Ergang (Ascom/SPR);

f) Juliana Nunes Batista de Lima França (Ascom/SPR); e

g) Rakell Cabral Dimanski (Ascom/SPR).

Art. 2º Esta portaria entra em vigor na data da publicação.

Ministra ROSA WEBER

Portaria nº 601 de 07 de agosto de 2019

Institui a Comissão Avaliadora para atuar no Teste Público de Segurança – 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 10 da Resolução-TSE nº 23.444 , de 30 de abril de 2015,

RESOLVE:

Art. 1º Instituir a Comissão Avaliadora para atuar na realização do Teste Público de Segurança - 2019, com a seguinte composição:

I - Dr. Rogério Augusto Viana Galloro, Assessor Especial, representante da Presidência do TSE;

II - membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:

a) Prof. Dr. Mamede Lima Marques;

b) Dr. Osvaldo Catsumi Imamura; e

d) Prof. Dr. Jamil Salem Barbar.

III - Dr. Luis Otávio de Colla Furquim, representante do Ministério Público Federal;

IV - Dr. José Rorilson Vieira Araújo, Analista de Desenvolvimento de Sistemas de Tecnologia da Informação do Conselho Federal da OAB; (Redação dada pela Portaria n° 920/2019)

V - Dr. Frederico Quadros D'Almeida, representante do Congresso Nacional;

VI - Dr. Marcelo Antonio da Silva, Perito Criminal Federal, representante do Departamento de Polícia Federal;

VII - Dr. Rodrigo de Souza Borges, representante do Conselho Federal de Engenharia e Agronomia; e

VIII - Prof. Paulo Lício de Geus, representante da Sociedade Brasileira de Computação.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Ministra ROSA WEBER

Portaria nº 920 de 22 de novembro de 2019

Altera a Portaria-TSE nº 601 de 7 de agosto de 2019, que institui a Comissão Avaliadora para atuar no Teste Público de Segurança – 2019.

A PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais e tendo em vista o contido no Ofício GPR nº 1562 de 22 de novembro de de 2019, subscrito pelo Presidente Nacional da Ordem dos Advogados do Brasil, Dr. Felipe Santa Cruz,

RESOLVE:

Art. 1º O inciso IV do art. 1º da Portaria-TSE nº 601 de 7 de agosto de 2019 passa a vigorar com a seguinte redação:

"Art. 1º .....

IV - Dr. José Rorilson Vieira Araújo, Analista de Desenvolvimento de Sistemas de Tecnologia da Informação do Conselho Federal da OAB; .....".

Art. 2º Esta portaria entra em vigor na data de sua publicação.

ROSA WEBER

Ministra

Anexo C – Lista de investigadores, de observadores e de apoio técnico

INVESTIGADORES

Alan Papafanurakis Heleno

Caio Henrique de Aquino

Charles William Biesseki

Fabio Rosindo Daher de Barros

Fellipe Ribeiro Silva Abib

Fernando Nogueira da Silva

Gabriel Cardoso de Carvalho

Gabriel Ferrari Carvalho

Galileu Batista de Sousa

Igor Palmieri Antunes

Ivo de Carvalho Peixinho

Jairo Simão Santana Melo

José Filippe de Moraes Albano

Josinei Rodrigues Lopes Silva

Leonardo Cunha dos Santos

Leonardo de Almeida Ramos

Luis Antonio Brasil Kowada

Luis Fernando de Almeida

Luiz Fernando Sirotheau Serique Junior

Paulo César Herrmann Wanner

Ramon Rocha Rezende

Victor Faria de Sousa

OBSERVADORES

Danilo Magno Marchiori – TRE/ES

Dory Gonzaga Rodrigues – TRE/GO

Gilmar Jose Fernandes de Deus – TRE/PR

José Cassimiro Júnior – TRE/PB

Vanderlan Fonseca dos Santos Junior – TRE/RR

APOIO TÉCNICO

Amandio Ferreira Balcão Filho – CTI

Dave Pinheiro – TRE/PA

Dilson Athias Mesquita – TRE/PA

Guilherme Cesar Soares Ruppert – CTI

José Augusto de Oliveira Neto – TRE/PB

Luciano Chapuis de Oliveira – TRE/MG

Luiz Angelo Daros de Luca – TRE/SC

Luiz Gustavo Marques Florindo – TRE/MG

Luiz Otávio Duarte – Facti

Mozart Fernandes Moreira Lima – TRE/MG

Ralph Werner Gomes Viegas – TRE/MG

Roberto Lopes Rocha – TRE/PA

Roger Gomes da Silva – TRE/MG

Anexo D – Resultado definitivo das inscrições

Camila Lúcia Pereira Rio

Título	Resumo	Resultado
Fraude na inicialização da votação.	A adoção de sistemas de informação em processos eleitorais trouxe benefícios, como a publicação mais rápida de resultados e a dificuldade na prática de algumas fraudes que dependem do processo manual. Por outro lado, pode introduzir novas vulnerabilidades que podem ser exploradas para a ocorrência de novos tipos de fraudes, até então inexistentes. O teste visa alterar o resultado de uma votação no início, ou seja, alterar as escolhas dos eleitores registradas pela urna.	Reprovado. O plano de teste apresentado dependia da utilização dos Sistemas Candidaturas e CANDex para a sua efetiva realização. No entanto, os referidos sistemas não são objeto de teste para o TPS 2019, conforme estabelecido no art. 2º do edital. "Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados."

Fellipe Ribeiro Silva Abib

Título	Resumo	Resultado
Manipulação do Boletim de Urna.	O teste a ser realizado busca conhecer o processo da geração dos Boletins de Urnas, além de apontar padrões, falhas e a ordem dos eleitores que votaram, para identificar quem votou em qual candidato.	Aprovado. A participação no TPS está pendente de complementação de informações. O grupo de investigadores deverá entrar em contato com o TSE para sanar a pendência.

Jairo Simão Santana Melo

Título	Resumo	Resultado
Teste da urna eletrônica baseado em IA e em processamento de sinais.	O escopo do presente plano é realizar avaliação sistêmica da atual configuração da urna eletrônica em uso no processo eleitoral brasileiro, buscando empregar técnicas de aprendizado de máquina e de captura de sinais elétricos em um ciclo de treinamento, teste e definição do percentual de acurácia em relação aos dados de entrada.	Aprovado. O grupo de investigadores deverá trazer osciloscópio e *notebook* para a realização do teste. No ambiente do teste, não há conexão com a internet, mas o grupo poderá acessá-la em outro ambiente. Os equipamentos utilizados no teste poderão ficar retidos, conforme prevê o inciso V do art. 40 do edital do TPS, segundo o qual os equipamentos, dispositivos eletrônicos e materiais citados nos incisos I, II e III deste artigo, quando aprovados, poderão ficar retidos no TSE por até 60 dias após o encerramento da realização do TPS.

José Filippe de Moraes Albano

Título	Resumo	Resultado
Exploração de vulnerabilidades na infraestrutura de rede, nos sistemas e nos ativos.	O objetivo da exploração de vulnerabilidades na infraestrutura e nos ativos que compõem a urna eletrônica é simular um ataque aos ativos do TSE. Se encontrada vulnerabilidade, investigar-se-á o impacto causado e os sistemas afetados, com a finalidade de encontrar soluções que possam mitigar os ataques, garantindo o exercício do voto sem sua violação, por meio dos pilares da segurança da informação: confidencialidade, integridade e disponibilidade da informação.	Aprovado com ressalvas. O edital do TPS, em seu art. 2º, estabelece os sistemas eleitorais objeto do teste. "Art. 2º Os sistemas eleitorais que serão objetos do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna e seus *softwares* embarcados." Dessa forma, o plano de teste deve realizar ataques apenas aos sistemas apresentados, não sendo permitida a realização de ataques à rede do TSE. Haverá ambiente de teste segregado preparado para o TPS, onde o investigador poderá realizar os testes previstos no plano de teste.

Leonardo Cunha dos Santos

Título	Resumo	Resultado
Teste de invasão utilizando análise instantânea de pulso elétrico.	O teste é constituído pelo uso de reconhecimento de padrões a partir da detecção de pulsos elétricos, com a finalidade de compreender comportamentos do equipamento durante a operação de voto.	Aprovado com ressalvas. A participação no TPS depende de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.

Luis Antonio Brasil Kowada

Título	Resumo	Resultado
Tentativa de obtenção de chaves criptográficas.	O teste visa avaliar se os procedimentos e o gerenciamento de chaves garantem a confidencialidade e a autenticação.	Aprovado.
Verificação das vulnerabilidades das bibliotecas do sistema.	O teste visa avaliar a possibilidade de alteração de bibliotecas ou explorar vulnerabilidades de bibliotecas de terceiros.	Aprovado. O grupo de investigadores deverá providenciar instalador para o sistema operacional Kali Linux.

Luís Fernando de Almeida

Título	Resumo	Resultado
Tentativa de mapeamento de rotina aleatória por meio de algoritmos de reconhecimento de padrão.	Para garantir a confidencialidade dos votos, a urna eletrônica utiliza o recurso de rotinas pseudoaleatórias para proporcionar que um voto seja armazenado em posições ao acaso dentro do arquivo. Atualmente, nota-se crescente aplicação de rotinas inteligentes baseadas em Machine Learning ao problema de reconhecimento de padrão. A literatura apresenta casos de sucesso dessas rotinas em problemas de regressão e em modelos preditivos. Diante desse contexto, o teste em questão pretende analisar a possibilidade de rotinas inteligentes serem capazes de criar modelo apto a mapear a geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.	Aprovado.

Paulo César Herrmann Wanner

Título	Resumo	Resultado
Extração de dados e configurações do *Kit* JE Connect.	Obter senhas e configuração da VPN a partir de mídia do JE Connect. Tentar se conectar diretamente à rede do TSE a partir dos dados obtidos. Verificar existência de vulnerabilidades no RecArquivos, utilizando técnicas de *fuzzing*. Verificar possibilidade de acesso direto ao banco de dados e às suas rotinas.	Aprovado. O grupo de investigadores deverá providenciar disco rígido ou HDD externo de tamanho compatível para copiar as imagens via interface USB/Sata e também instalador para o sistema operacional Kali Linux.
Extração do conteúdo do disco criptografado do SIS.	Obter acesso físico ao disco do computador com o Gedai instalado para retirar o disco criptografado e buscar a chave no registro do Windows. Inicializar o disco em uma máquina virtual para obter *dump* de memória. Extrair a chave a partir do *dump* e comparar com as informações obtidas no registro para estabelecer processo de formação da chave. Montar o disco cifrado e extrair os dados nele presentes. Verificar, no disco cifrado, informações sensíveis para o processo eleitoral.	Aprovado. O TSE providenciará material para abertura do gabinete do computador a ser utilizado no plano de teste. O grupo de investigadores deverá providenciar o disco rígido ou HDD externo de tamanho compatível para copiar as imagens via interface USB/Sata e mídia removível de alta capacidade (64 GB ou superior).
Instalação e execução de código arbitrário em uma máquina do Gedai para implante de dados falsos na urna eletrônica.	Obter acesso físico ao computador com o Gedai instalado para fazer imagem completa do disco. Inicializar o disco em uma máquina virtual. Subverter o sistema de inicialização para viabilizar o *boot* sem a carga do SIS. Acessar e modificar programas de criação e preparação de dados a serem gravados nas urnas eletrônicas. Criar cartão de inicialização da urna com dados espúrios.	Aprovado. O TSE providenciará material para abertura do gabinete do computador a ser utilizado no plano de teste. O grupo de investigadores deverá providenciar o disco rígido ou HDD externo de tamanho compatível para copiar as imagens via interface USB/Sata e mídia removível de alta capacidade (64 GB ou superior).

Roberto Miyano Neto

Título	Resumo	Resultado
CT001 – Integridade do arquivo executável da urna – Vota.	Verificar se o arquivo executável assinado somente é executado após verificação da assinatura.	Aprovado com ressalvas. A participação no TPS depende de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.

Título	Resumo	Resultado
CT002 – Integridade da coleta de votos.	Verificar se o processo de coleta de votos gera provas de integridade para cada voto, obedecendo aos requisitos funcionais de sigilo do voto, definidos pela Constituição brasileira.	Aprovado com ressalvas. A participação no TPS depende de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.
Integridade do arquivo de votos.	Verificar se o arquivo de votos contém a lista de votantes e os votos armazenados fora de ordem, garantindo o sigilo constitucional, porém com provas de integridade por voto e com integridade entre a quantidade de votantes e votos. Verificar ainda se tal arquivo é assinado com chave privada única por urna, conhecida pelo TSE, armazenada em HSM.	Aprovado com ressalvas. A participação no TPS depende de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.

Anexo E – Planos de teste dos participantes

Grupo 1

Manipulação do boletim de urna

Informações gerais

Resumo do teste:

O teste a ser realizado será conhecer o processo da geração dos boletins de urnas, identificar padrões, identificar as falhas, abrir o boletim e identificar a ordem dos eleitores que votaram para saber quem votou em qual candidato.

Sistemas afetados

Softwares: Software básico de urna eletrônica, Aplicativos da urna eletrôncia, Sistemas de transmissão e recebimento de arquivos de urna eletrônica
Hardwares: Urna eletrônica, Transmissão de arquivos (Kit JE Connect)
Procedimentos: Votação, Transmissão de arquivos

Detalhamento do teste

1. Descrição geral do teste

O teste a ser realizado é a identificação do eleitor dentro do boletim de urna, caso não possua os dados do eleitor dentro do boletim, identificar a ordem da votação. Terá tentativa de falsificar o boletim de urna para o envio e manipular a eleição com dados que será fornecido no boletim falso. Poderá ocorrer outros testes à medida que for conhecendo e familiarizando com o sistema.

2. Fundamentação teórica

Os dados armazenados no flash das memorias de armazenamento possui as informações do candidato que o eleitor votou, portanto, é possível identificar a ordem e descobrir o candidato votado por cada eleitor através dos logs e histórico de gravação.

3. Precondições para o teste

Uma urna com dados já carregados e encerrada a votação.

4. Escopo – Superfície do ataque

Será estudado a geração do boletim de urna, sua geração, e por consequência sua gravação até a transmissão do boletim para ser computado.

5. Janela de atuação simulada do atacante

Uma urna comum que após as eleições e geração do boletim de urna, antes de ser enviado será atacado para enviar o boletim falso.

6. Pontos de intervenção

Geração do BU pela urna eletrônica e o processo de transmissão.

7. Passos a serem realizados

Saber como é gerado o BU inicial, conhecer os dados armazenados, identificar os eleitores e seus votos, reconhecer sua criptografia e refazer esse passo em um novo BU modificado pela equipe.

8. Material necessário

2 Computadores com Windows 10 Pro 1903 (x64) com os seguintes softwares: IDA pro (versão 70+), nmap, sysinternals, FTK Imager, netcat, fake path, metaexploit framework, winscp, Windows SubSistema Linux instalado com Ubuntu e Kali instalado, Fakenet, Wireshark, OBDG110 ou superior, Resource Hacker, 1 Computador com Kali (x64) versão 2019.3 e 1 computador com Caine 10.0+.

9. Possíveis resultados e impacto

Identificação do eleitor e o candidato votado, o que na constituição é proibido.

10. Rastreabilidade

Se obtivermos sucesso será possível manipular uma eleição tendo acesso direto com o software de transmissão com o objetivo de mandar um BU manipulado.

11. Solução proposta

Não armazenar o log e não gravar os dados do eleitor no boletim de urna.

Grupo 2

Teste da urna Eletrônica baseado em IA e Processamento de Sinais

Informações gerais

Resumo do teste:

Escopo do presente plano busca abordar uma avaliação sistêmica da atual configuração da urna eletrônica em uso no processo eleitoral brasileiro, buscando empregar técnicas de aprendizado de máquina e captura de sinais elétricos em um ciclo de treinamento, teste e definição do percentual de acurácia em relação aos dados de entrada.

Sistemas afetados

Softwares: Software básico de urna eletrônica, Aplicativos da urna eletrôncia
Hardwares: Urna eletrônica
Procedimentos: Votação

Detalhamento do teste

1. Descrição geral do teste

O seguinte teste ira contemplar aspectos de hardware e software sobre o seguinte fluxo:

i) A equipe de teste ao recepcionar a urna fornecida pelo TSE, a mesma será aberta com a finalidade de que os sinais [2] de entrada possam ser capturas por um osciloscópio.

ii) Após a captura dos sinais produzidos por todas as teclas do teclado, a respectiva coleta será exportada para um arquivo em formato UTF.

iii) Esse arquivo será tratado removendo possíveis interferências;

iv) Após a normalização, esse arquivo será submetido a um algoritmo de clusterização [3] escrito me Python [1], buscando identificar a formação de um certo conjunto de família de dados. Essas famílias devem buscar representar sinal de cada tecla do teclado, mesmo que o sinal esteja modulado por uma chave de criptografia a representação de similaridade do sinal retirando a portadora será a mesma.

v) Será gerado um segundo arquivo, a fim de validar a acurácia gerada no treinamento.

vi) Ao final será gerando um relatório e entregue a instituição.

2. Fundamentação teórica

O presente trabalho fundamenta-se na ideia de que os sinais da urna possam ser recuperados por um ***osciloscópio [1],*** *e mesmo que criptografado com um senha master, o aprendizado de máquina pode clusterizar as teclas da urna.*

[1] https://teses.usp.br/teses/disponiveis/55/55134/tde-06102003-160219/publico/TeseDoutorado.pdf

3. Precondições para o teste

1º Acesso a urna de votação sem lacres com qualquer restrição ao hardware.

4. Escopo – Superfície do ataque

Verificar a viabilidade de recuperar os sinais gerados pelo teclado da urna eletrônica e submete-los a um algoritmo de classificação.

5. Janela de atuação simulada do atacante

Durante o processo de votação.

6. Pontos de intervenção

Durante o processo de votação os respectivos sinais do teclado serão capturados e repassados ao algoritmo de classificação.

7. Passos a serem realizados

O seguinte teste ira contemplar aspectos de hardware e software sobre o seguinte fluxo:

i) A equipe de teste ao recepcionar a urna fornecida pelo TSE, a mesma será aberta com a finalidade de que os sinais [2] de entrada possam ser capturas por um osciloscópio.

ii) Após a captura dos sinais produzidos por todas as teclas do teclado, a respectiva coleta será exportada para um arquivo em formato UTF.

iii) Esse arquivo será tratado removendo possíveis interferências;

iv) Após a normalização, esse arquivo será submetido a um algoritmo de clusterização [3] escrito me Python [1], buscando identificar a formação de um certo conjunto de família de dados. Essas famílias devem buscar representar sinal de cada tecla do teclado, mesmo que o sinal esteja modulado por uma chave de criptografia a representação de similaridade do sinal retirando a portadora será a mesma.

v) Será gerado um segundo arquivo, a fim de validar a acurácia gerada no treinamento.

vi) Ao final será gerando um relatório e entregue a instituição.

8. Material necessário

1 Urna Eletrônica padrão TSE	Urna eletrônica com as configurações da última eleição sem lacres de segurança.
1 notebook	I7, com 32 GB de RAN e disco SSD 128 + HD 1TB, com S.O Windows 10 instalado, compilador python e IDE paycharm. O mesmo deve possuir entrada USB e conexão com a internet.

9. Possíveis resultados e impacto

* Ser possível recuperar os dados digitados pelo usuário da urna.

10. Rastreabilidade

* ser possível gerar o código votante

11. Solução proposta

*** Chave de criptográfia de sessão reduzida.

Grupo 3

Tentativa de obtenção de chaves criptográficas

Informações gerais

Resumo do teste:

Este teste visa avaliar se os procedimentos e gerenciamento de chaves garantem a confidencialidade e autenticação.

Sistemas afetados

Softwares: Software Desktop para preparação de mídia de urna eletrônica, Software básico de urna eletrônica, Aplicativos da urna eletrôncia
Hardwares: Urna eletrônica
Procedimentos: Geração de mídias, Carga da urna, Votação

Detalhamento do teste

1. Descrição geral do teste

O teste consiste em analisar todas as etapas em que os dados são cifrados ou autenticados.
Em paralelo é observado se as chaves criptográficas são armazenadas corretamente pela CriptoTable.

2. Fundamentação teórica

Para que um sistema criptográfico funcione como se espera, é necessário que as partes autorizadas possuam as chaves criptográficas de decodificação, e apenas elas. Isto significa que dependendo de como as chaves são armazenadas, é possível um intruso (parte não autorizada) ter acesso a informações confidenciais. Por isso é importante o conhecimento de como as chaves são guardadas.
Outra condição necessária para o bom funcionamento do sistema criptográfico é que ele tenha sido implementado corretamente.
Uma possibilidade de ataque é a substituição do código-executável legítimo por um malicioso. Mas mesmo o código legítimo pode conter brechas de segurança por alguma falha de implementação (por exemplo, não contemplar todas as exceções).

3. Precondições para o teste

Conhecimento das diversas etapas do processo de alimentação de programas e dados nas urnas.
Conhecimento dos algoritmos criptográficos envolvidos.
Conhecimento do código-fonte.

4. Escopo – Superfície do ataque

O ataque será realizado sobre os procedimentos de cifragem e autenticação dos sistemas GEDAI-UE, SCUE, GAP, VOTA, RED e SA entre outros.

5. Janela de atuação simulada do atacante

Caso a vulnerabilidade seja encontrada no GEDAI-UE, o atacante precisa ter acesso aos servidores da origem das informações (supostamente no TSE), ou ao canal de transmissão (no qual as informações são trafegadas via SFTP) ou ao destino (servidores que alimentarão as informações das urnas). Caso a vulnerabilidade seja no SCUE, o atacante precisa ter acesso também a algum dos agentes envolvidos na comunicação (servidor ou urna).
Nos outros sistemas, se houver vulnerabilidade, o ataque será feito sobre a urna.

6. Pontos de intervenção

Devido à grande abrangência do ataque, o atacante pode atuar em diversas etapas do processo como Preparação, Geração de Mídias ou Carga das Urnas.

7. Passos a serem realizados

1) Análise da alimentação dos dados sobre candidatos, seções e eleitores nos servidores através do sistema GEDAI-UE.
2) Análise da alimentação dos dados sobre candidatos, seções e eleitores nas urnas através do software de carga SCUE.
3) Análise da manipulação destas informações pelo GAP, VOTA, RED e SA.

8. Material necessário

Os materiais e equipamentos previstos no edital.

9. Possíveis resultados e impacto

Os possíveis resultados são o uso incorreto dos algoritmos criptográficos e no armazenamento das chaves criptográficas envolvidas no processo. Caso isso ocorra, pode-se descobrir como alterar algum dos procedimentos envolvidos.

10. Rastreabilidade

A detecção de uma possível fraude depende de qual sistema foi atingido.

11. Solução proposta

A solução depende do resultado da análise. Caso seja encontrada uma vulnerabilidade no uso dos procedimentos criptográficos, podem ser propostas alterações no modo de uso.

Verificar vulnerabilidades das bibliotecas do sistema

Informações gerais

Resumo do teste:

Este teste visa avaliar a possibilidade de alteração de bibliotecas ou explorar vulnerabilidades de bibliotecas de terceiros.

Sistemas afetados

Softwares: Software Desktop para preparação de mídia de urna eletrônica, Software básico de urna eletrônica, Aplicativos da urna eletrôncia
Hardwares: Urna eletrônica
Procedimentos: Geração de mídias, Carga da urna, Votação

Detalhamento do teste

1. Descrição geral do teste

O teste consiste em conhecer quais são as bibliotecas usadas no sistema. Procurar vulnerabilidades nelas. Caso seja descoberta a chave de cifragem de bibliotecas, tentar alterar o conteúdo das mesmas.

2. Fundamentação teórica

Um sistema que faz uso de bibliotecas externas pode conter vulnerabilidades não somente em seu código fonte mas também pode trazer nas bibliotecas de que faz uso, sendo assim podem existir falhas que não necessitem alteração de código para serem exploradas. Além disso, uma vez encontradas as chaves de criptografia será possível descriptografar o kernel e fazer uma análise mais detalhada. No caso de existir conteúdo não assinado pelo sistema poderão ser feitas alterações no código não assinado, uma vez que poderíamos descriptografar o conteúdo, alterá-lo e criptografar novamente.

3. Precondições para o teste

Conhecimento das diversas etapas do processo de alimentação de programas e dados nas urnas.

Conhecimento das bibliotecas usadas no sistema.

Conhecimento do código-fonte.

Conhecimento de vulnerabilidades de bibliotecas de terceiros.

4. Escopo – Superfície do ataque

O ataque será realizado sobre os procedimentos de cifragem e autenticação dos sistemas GEDAI-UE, SCUE, GAP, VOTA, RED e SA entre outros.

5. Janela de atuação simulada do atacante

Caso a vulnerabilidade seja encontrada no GEDAI-UE, o atacante precisa ter acesso aos servidores da origem das informações (supostamente no TSE), ou ao canal de transmissão (no qual as informações são trafegadas via SFTP) ou ao destino (servidores que alimentarão as informações das urnas). Caso a vulnerabilidade seja no SCUE, o atacante precisa ter acesso também a algum dos agentes envolvidos na comunicação (servidor ou urna).

Nos outros sistemas, se houver vulnerabilidade, o ataque será feito sobre a urna.

6. Pontos de intervenção

Devido à grande abrangência do ataque, o atacante pode atuar em diversas etapas do processo como Preparação, Geração de Mídias ou Carga das Urnas.

7. Passos a serem realizados

1 - Engenharia reversa no kernel para tentativa de recuperação de chaves criptográficas.

2 - Busca de vulnerabilidades aplicáveis em bibliotecas externas.

3 - Busca de conteúdo não assinado.

4 - Em caso de existência de conteúdo não assinado e de as chaves criptográficas serem encontradas haverá a tentativa de alteração de código.

8. Material necessário

Se possível, gostaríamos que o microcomputador disponibilizado para a equipe possua o Linux Kali.

9. Possíveis resultados e impacto

Os possíveis resultados dependem de quais bibliotecas são vulneráveis.

10. Rastreabilidade

A detecção de uma possível fraude depende de qual sistema foi atingido.

11. Solução proposta

A solução depende do resultado da análise. Caso seja encontrada uma vulnerabilidade no uso dos procedimentos criptográficos, podem ser propostas alterações no modo de uso.

Grupo 4

Tentativa de mapeamento de rotina aleatória por meio de algoritmos de reconhecimento de padrão

Informações gerais

Resumo do teste:

Para fins de garantir a confidencialidade dos votos, sua na urna eletrônica utiliza do recurso de rotinas pseudo-aleatórias para proporcionar que um voto seja armazenado em posições ao acaso dentro do arquivo. Atualmente, nota-se a crescente aplicações de rotinas inteligente baseadas em Machine Learning aplicadas ao problema de Reconhecimento de Padrão. A literatura apresenta casos de sucesso desta rotinas em problemas de regressão e modelo preditivos. Diante deste contexto, o teste em questão pretende analisar a possibilidade de rotinas inteligente serem capazes de criarem um modelo capaz de mapear a geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

Sistemas afetados

Softwares: Aplicativos da urna eletrôncia
Hardwares: Urna eletrônica
Procedimentos: Votação

Detalhamento do teste

1. Descrição geral do teste

O teste em questão baseia-se na tentativa de se criar um modelo preditivo que seja capaz de mapear a rotina aleatória utilizada para geração dos números que serão utilizados para determinar a posição do voto dentro do arquivo. O estudo pretende, a partir de uma determinada sequências de número geradas por esta rotina aleatória, submeter a algoritmos de Machine Learning e verificar a possibilidade destes detectarem a sequência de número gerada, ou seja, a posição de cada voto armazenado no respectivo arquivo de votos. Desta forma, será possível identificar a posição do voto do primeiro eleitor, do segundo eleitor e assim sucessivamente.

2. Fundamentação teórica

O reconhecimento de padrão, dentre as diversas definições apresentadas pela literatura, pode ser definido como um problema cujo objetivo é a classificação de objetos em um número de categorias ou classes e, dependendo da situação, estes objetos pode ser imagens ou sinais de ondas ou qualquer tipo de medida que necessita ser classificada. O reconhecimento de padrão envolve algumas tarefas: classificação, agrupamento, regressão, previsão, dentre outras. Destas, observa-se a tarefa de regressão, que é uma tarefa preditiva onde a variável alvo a ser avaliada é contínua, podendo ser um número real ou inteiro. A literatura apresenta casos de sucesso com relação a aplicação de técnicas para modelos preditivos baseados em aplicação de algoritmos para tarefas de regressão.

3. Precondições para o teste

Para execução do teste é necessário:

- acesso ao código fonte que descreve a rotina aleatória atual para entendimento do procedimento para geração da semente da rotina aleatória.

- urna eletrônica para simulação de eleição com a relação de eleitores cadastrado para esta urna.

- acesso ao arquivo com os registros do votos, com a posição onde cada um foi gravado após conclusão da eleição.

4. Escopo – Superfície do ataque

O teste envolve o software de votação da urna eletrônica, especificamente, o módulo o qual registra os votos nas tabelas/arquivos de voto. O ataque visa analisar a qualidade da rotina aleatória utilizada quanto à possibilidade de de mapeamento por meio de técnicas de Machine Learning.

5. Janela de atuação simulada do atacante

O ataque durante a votação da seguinte forma:

- No momento que cada eleitor vota, registra-se a sequência de quem está votando, supostamente, por alguém que esteja presenta na seção.

- Em paralelo, partindo do princípio da possibilidade de criação do modelo de geração dos número aleatórios, o programa registra onde este voto será gravado no arquivo.

- Ao final da eleição tem-se duas listas: uma primeira com a sequência cronológica dos eleitores; uma segunda, a sequência da posição onde os votos foram gravados.

6. Pontos de intervenção

Durante a votação seria registrado a sequência dos eleitores que estão votando, por agente externo presente na seção eleitoral e, após o fechamento da urna, com o acesso a mídia de votos, o mapeamento da posição do voto de cada eleitor dentro deste arquivo.

7. Passos a serem realizados

1. Codificação de algoritmos de Machine Learning (ML) para modelos preditivos.

2. Simulação de votação utilizando urna eletrônica.

2.1 Essa simulação será da seguinte forma: primeiro voto para o candidato 1, segundo voto para o candidato 2, até o voto 99, do eleitor 99. Após isso gera o BU da urna.

2.2 Fazer esta simulação mais de uma vez, inicialmente, 5 vezes.

3. Analisar código fonte para analisar o procedimento para geração da semente da rotina aleatória

4. Submeter o arquivo de dados para os algoritmos para verificar a possibilidade de se criar o modelo da rotina aleatória.

5. Obtido sucesso, executar nova simulação em paralelo com o programa para verificar se é possível predizer a posição de gravação de cada voto.

8. Material necessário

1. 02 Computadores com compilador C e Python.

2. 02 urnas eletrônicas preparadas para votação.

3. Acesso ao código fonte da urna eletrônica: especificamente, módulo de gravação de votos e rotina aleatória.

4. Acesso livre ao conteúdo do arquivo de votos da urna da votação simulada.

9. Possíveis resultados e impacto

O êxito to teste resulta na possibilidade da quebra do sigilo do voto visto que seria possível associar cada voto a cada eleitor.

10. Rastreabilidade

A detecção da efetividade do ataque somente poderia ser realizada por meio de uma simulação imediata do TSE de uma votação em comparação com o programa de mapeamento de gravação dos votos.

11. Solução proposta

Aperfeiçoamento da rotina aleatória, algoritmo, geração da semente, para evitar seu mapeamento por meio de algoritmos inteligentes.

Grupo 5

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Extração de dados e configurações do Kit JE Connect	
Instituição proponente (se aplicável) Polícia Federal	
Responsável Paulo César Herrmann Wanner	
Resumo do teste (máximo de 120 caracteres) 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 existência de vulnerabilidades no RecArquivos utilizando técnicas de fuzzing 4. Verificar possibilidade de acesso direto ao banco de dados e as suas rotinas.	
Sistemas afetados *Softwares* ( ) *Software Desktop* para preparação de mídia de urna eletrônica ( ) *Software* básico da urna eletrônica ( ) Aplicativos da urna eletrônica (X) Sistemas de transmissão e recebimento de arquivos de urna eletrônica ( ) Subsistema de Instalação e Segurança (SIS)	*Hardwares* ( ) Urna eletrônica (X) Transmissão de arquivos (*Kit* JE Connect) Procedimentos ( ) Geração de mídias ( ) Carga da urna ( ) Votação (X) Transmissão de arquivos

1 – Descrição geral do teste

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

2 – Fundamentação teórica
O JE Connect possui as configurações para acesso via VPN a rede do TSE. Acredita-se que seja possível obter a configuração da VPN e possíveis credenciais existentes no Kit JE Connect via dados do sistema de arquivos ou dump de memória.

3 – Precondições para o teste
Estação com Kali Linux e kit JE Connect.
Ferramentas para virtualização (QEMU/virtualbox), duplicação de dados (dd/ddrescue), montagem de sistema de arquivos (mount), análise de dump de memória (volatility) e openvpn.

4 – Escopo – Superfície de ataque
Kit JE Connect, VPN, RecArquivos.

5 – Janela de atuação simulada do atacante
Acesso ao Kit JE Connect.

6 – Pontos de intervenção
Mídia JE Connect
VPN

7 – Passos a serem realizados
Material necessário:

- Kit JE Connect
- Estação com Kali Linux para duplicação e montagem do sistema de arquivos da mídia do JE Connect
- Programas para análise de memória, duplicação de dados e montagem de sistemas de arquivos.
- Programas para virtualização Virtualbox e QEMU
- Programa para análise de tráfego de rede (tcpdump, wireshark)
- Programa openvpn
- Programas OWASP WSFuzzer, Burp Suite Community Edition e fuzzapi

Passos:

1. Realizar imagem da mídia JE Connect
2. Inicialização a mídia JE Connectc em um ambiente virtualizado para realizar um *dump* de memória
3. Montagem dos dados existente no sistema de arquivos a fim de identificar credenciais e configuração da VPN
4. Caso seja possível obter tais informações, estabelecer uma conexão via VPN e testar o recebimento de arquivos utilizando técnicas fuzzing

8 – Materiais necessários (fornecidos pelo TSE)
Estação Kali Linux com ferramentas necessárias
Disco rígido ou HDD externo USB de tamanho compatível para copiar as imagens
Interface USB / SATA

9 – Possíveis resultados e impacto
Em um ataque bem-sucedido seria possível obter acesso a rede privada do TSE, acessar o RecArquivos e o banco de dados do Totalizador

10 – Rastreabilidade

11 – Solução proposta

Protocolo	Data 22/10/2019
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Extração do conteúdo do disco criptografado do SIS	
Instituição proponente (se aplicável) Polícia Federal	
Responsável Paulo César Herrmann Wanner	
Resumo do teste (máximo de 120 caracteres) 1. Obter acesso físico ao disco do computador com o GEDAI instalado para retirar o disco criptografado e buscar a chave no registro do Windows. 2. Inicializar o disco em uma máquina virtual para obter um *dump* de memória. 3. Extrair a chave a partir do *dump* e comparar com as informações obtidas no registro para estabelecer processo de formação da chave. 4. Montar o disco cifrado e extrair os dados presentes neste disco. 5. Verificar no disco cifrado informações sensíveis para o processo eleitoral.	
Sistemas afetados *Softwares* (X) *Software Desktop* para preparação de mídia de urna eletrônica ( ) *Software* básico da urna eletrônica ( ) Aplicativos da urna eletrônica ( ) Sistemas de transmissão e recebimento de arquivos de urna eletrônica (X) Subsistema de Instalação e Segurança (SIS)	*Hardwares* ( ) Urna eletrônica ( ) Transmissão de arquivos (*Kit* JE Connect) Procedimentos ( ) Geração de mídias ( ) Carga da urna ( ) Votação ( ) Transmissão de arquivos

1 – Descrição geral do teste

O teste visa verificar a possibilidade de extração de informações sensíveis dentro do volume cifrado usado pela biblioteca SIS para armazenar os programas usados pelo sistema eleitoral, como o GEDAI. Acredita-se que hajam informações sensíveis neste volume como por exemplo chaves privadas de criptografia que são alimentadas nas urnas eletrônicas através do programa GEDAI.

2 – Fundamentação teórica

A partir de análises do código fonte, verificou-se que o SIS cria um volume criptografado a partir de uma chave gerada dinamicamente usando bibliotecas padrão do Windows para geração de GUID e uso de funções *hash*. Acredita-se que seja possível obter essa chave ou pela análise do local onde a chave é armazenada (Registro do Windows) ou pelo *dump* de memória e busca usando programas como Volatility, Rekall e AESFIND.

3 – Precondições para o teste

Estação Windows com SIS e GEDAI-UE instalado e com disco criptografado gerado.

Ferramental que permita abrir o desktop para extração do disco ou CD *live* para realização de cópia forense do disco.

Ferramentas de análise de registro, dump de memória e busca de chaves.

4 – Escopo – Superfície de ataque

Estação desktop com SIS instalado e programas como GEDAI e Transportador.

5 – Janela de atuação simulada do atacante

Acesso físico ao computador onde foram geradas as mídias.

6 – Pontos de intervenção

Sistema SIS

Sistema Operacional Windows

Disco criptografado gerado pelo sistema SIS

7 – Passos a serem realizados

Material necessário:

- Estação com o GEDAI-UE instalado e o sistema SIS com o disco criptografado gerado e montado
- Ferramenta para retirada do disco ou CD live para inicialização de um sistema operacional alternativo
- Mídia removível de pelo menos 64gb para cópia dos arquivos
- Ferramenta (chave phillips) para abertura do gabinete caso não seja possível a cópia na própria estação.
- CD com programas para análise de memória (volatility / rekall), análise do registro do Windows (hivexsh), FINDAES para busca de chaves de criptografia e Truecrypt para montagem do disco.
- Interface USB para disco rígido SATA
- Virtualbox e QEMU para virtualização

Passos:

1. Inicialização com LIVE CD para cópia do disco cifrado e dump do registry do Windows para mídia removível
2. Caso o primeiro passo não seja possível ler o disco diretamente via interface USB
3. Montagem do disco cifrado usando as informações do registro do Windows e o programa Truecrypt
4. Caso o não seja possível montar o disco, realizar cópia e inicialização em uma máquina virtual para fazer *dump* de memória
5. Análise e extração da chave em memória com as ferramentas apropriadas
6. Montagem do disco cifrado e cópia dos arquivos sensíveis.

8 – Materiais necessários (fornecidos pelo TSE)

Ferramenta para abertura de gabinete

Disco rígido ou HDD externo USB de tamanho compatível para copiar as imagens

Interface USB / SATA

Mídia removível de alta capacidade (64gb ou superior)

9 – Possíveis resultados e impacto

Em um ataque bem-sucedido seria possível obter dados sensíveis da estação de geração das mídias como chaves de criptografia

10 – Rastreabilidade

O rompimento de lacres da estação poderia evidenciar que a mesma foi violada e os dados sensíveis copiados.

11 – Solução proposta

Protocolo	Data 22/10/2019
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Instalação e execução de código arbitrário em uma máquina do GEDAI para implante de dados falsos na Urna Eletrônica.
Instituição proponente (se aplicável) Polícia Federal
Responsável Paulo César Herrmann Wanner
Resumo do teste (máximo de 120 caracteres) 1. Obter acesso físico ao computador com o GEDAI instalado para fazer uma imagem completa do disco. 2. Inicializar o disco em uma máquina virtual. 3. Subverter o sistema de inicialização para viabilizar o boot sem a carga do SIS. 4. Acesso e modificação de programas de criação e preparação de dados a serem gravados nas urnas eletrônicas. 5. Criar um cartão de inicialização da urna com dados espúrios.

Sistemas afetados	
Softwares (X) *Software Desktop* para preparação de mídia de urna eletrônica ( ) *Software* básico da urna eletrônica ( ) Aplicativos da urna eletrônica ( ) Sistemas de transmissão e recebimento de arquivos de urna eletrônica (X) Subsistema de Instalação e Segurança (SIS)	*Hardwares* ( ) Urna eletrônica ( ) Transmissão de arquivos (*Kit* JE Connect) Procedimentos ( ) Geração de mídias ( ) Carga da urna ( ) Votação ( ) Transmissão de arquivos

1 – Descrição geral do teste

O teste visa verificar a possibilidade de instalação e modificação de arquivos e programas na máquina em que o GEDAI executa. Dessa forma, uma parte do processo descentralizado nos TREs poderia ser comprometido e informações falsas sobre candidatos, por exemplo, alimentadas nas urnas eletrônicas através do programa GEDAI.

2 – Fundamentação teórica

A partir de análises e de informações sobre a segurança nas máquinas do GEDAI, nos permitem inferir que toda a segurança se baseia no endurecimento de todos os critérios de segurança do sistema Windows, que passam a ser, na maior parte, controladas pelo SIS. A desativação do SIS e a modificação nos demais programas usados na geração de informações para carga na URNA poderia proporcionar que as informações de eleitores e candidatos presentes no momento da votação fossem diferentes das reais.

3 – Fundamentação teórica

A partir de análises e de informações sobre a segurança nas máquinas do GEDAI, nos permitem inferir que toda a segurança se baseia no endurecimento de todos os critérios de segurança do sistema Windows, que passam a ser, na maior parte, controladas pelo SIS. A desativação do SIS e a modificação nos demais programas usados na geração de informações para carga na URNA poderia

proporcionar que as informações de eleitores e candidatos presentes no momento da votação fossem diferentes das reais.

4 – Precondições para o teste
Estação Windows com SIS e GEDAI-UE instalado.
Estação de trabalho com Windows 64 bits instalado e as seguintes ferramentas:

- Virtualbox instalado;
- Ferramental que permita a realização de cópia forense do disco (FTK Imager);
- Binários do BusyBox disponíveis;
- Imagem ISO do HIREN´s bootCD disponível;
- Ferramentas de debugger: Ollydbg e Xdbg (versões 32 e 64 bits) disponíveis.

5 – Escopo – Superfície de ataque
Estação desktop com SIS instalado e programas como GEDAI e demais utilitários.

6 – Janela de atuação simulada do atacante
Acesso físico ao computador onde foram geradas as mídias.

7 – Pontos de intervenção
Sistema SIS
Sistema Operacional Windows – especialmente o processo de inicialização e login de usuários;
Programas apoio à criação do cartão de memória para uso na Urna Eletrônica;
Disco criptografado gerado pelo sistema SIS

8 – Passos a serem realizados
Material necessário:

- Estação com o GEDAI-UE instalado e o sistema SIS com o disco criptografado gerado e montado
- Ferramenta para retirada do disco ou CD live para inicialização de um sistema operacional alternativo
- Ferramenta para cópia forense FTK Imager
- Mídia removível de pelo menos 64gb para cópia dos arquivos
- Ferramenta (chave phillips) para abertura do gabinete caso não seja possível a cópia na própria estação.
- CD com programas para análise, modificação de programas e sistema operacional: VirtualBox, HIRENS BootCD (imagens ISO: versões 15.2 e Pex64v1.0.1), BusyBox for windows 1.31.0-static, Ollydb v1.10 32bits, Ollydbg v2.01-64bit, xd64bg (versões 32bit e 64bit).
- Interface USB para disco rígido SATA

Passos:

1. Inicialização da máquina do GEDAI com LIVE CD para geração da imagem do disco para a mídia removível;
2. Carga da Imagem do GEDAI no Virtualbox como mídia secundária do HIREN´s BootCD.
3. Alterações no Registry do disco do GEDAI usando as ferramentas do HIREN´s, com objetivo de suplantar a carga do SIS durante do boot pela imagem principal do GEDAI;
4. Boot sem SIS na imagem principal do GEDAI;
5. Alteração de aplicações que geram dados para a urna eletrônica;
6. Verificação de implantação de dados falsos na Urna Eletrônica.

9 – Materiais necessários (fornecidos pelo TSE)
Ferramenta para abertura de gabinete

10 – Rastreabilidade

Discrepância entre dados de candidatos e/ou eleitores na urna eletrônica e nos sistemas do TSE.

11 – Solução proposta

Protocolo	Data 22/10/2019
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Exploração de vulnerabilidades na infraestrutura de rede, sistemas e ativos

Informações gerais

Resumo do teste:

O objetivo da exploração de vulnerabilidades na infraestrutura e nos ativos que compõe a urna eletrônica, tem como principal finalidade simular um ataque aos ativos do TSE.

Em caso positivo de encontrar a vulnerabilidade, investigar qual o impacto e os sistemas que podem ser afetados, bem como encontrar soluções que possam mitigar os ataques, garantindo o exercício do voto sem ocorrer a sua violação, através dos pilares da segurança da informação, que são eles: a confidencialidade, integridade e disponibilidade da informação.

Sistemas afetados

Softwares: Software Desktop para preparação de mídia de urna eletrônica, Software básico de urna eletrônica, Aplicativos da urna eletrônica, Sistemas de transmissão e recebimento de arquivos de urna eletrônica, Subsistema de Instalação e Segurança (SIS)
Hardwares: Urna eletrônica, Transmissão de arquivos (Kit JE Connect)
Procedimentos: Geração de mídias, Carga da urna, Votação, Transmissão de arquivos

Detalhamento do teste

1. Descrição geral do teste

O objetivo do teste, visa de uma maneira geral, encontrar falhas nos sistemas operacionais, seus aplicativos, softwares e em sua rede, afim de que possa ser investigado a sua maturidade de segurança e caso seja possível, explorar essas vulnerabilidades com o objetivo de alterar e fragilizar os votos na urna eletrônica.

2. Fundamentação teórica

A primeira etapa do teste, tem como objetivo coletar o máximo de informações sobre todo ambiente que será testado.

O método de coleta é chamado de footprint, onde será possível identificar os endereços de ips, blocos de rede, domínios, informações de usuários, versão dos aplicativos, sistemas, e todos os ativos da rede.

A segunda etapa do teste, é o de scanning, na onde será possível realizar o levantamento detalhado de hosts, protocolos, sistemas, aplicativos, análise de códigos fonte e tudo aquilo que envolvem o ambiente.

Isso poderá ser feito, através de scripts específicos de “scanning” ou até mesmo, na criação ou utilização de ferramentas específicas, que podem surgir durante o teste.

A terceira etapa, tem como objetivo explorar as falhas identificadas na etapa de scanning, afim de encontrar falhas que possam comprometer os pilares da segurança da informação, que é a sua confidencialidade, integridade e disponibilidade.

Essa etapa será onde será realizados ataques de buffer overflow, de exploits, injeção de códigos maliciosos, de escalação de privilégios, ataque de senhas e de outros que possam surgir, conforme o resultado das etapas anteriores.

3. Precondições para o teste

Para existir o teste é necessário o acesso a urna eletrônica, ao JE e aos endereços de rede que compõe os sistemas operacionais com as suas estações de trabalho e ao servidor do TSE.

4. Escopo – Superfície do ataque

O teste será realizado em toda infraestrutura e os sistemas que envolvem a urna eletrônica, como os sistemas operacionais, os sistemas de transmissão, os serviços e protocolos, os softwares e toda rede disponibilizada para os investigadores.

5. Janela de atuação simulada do atacante

O ataque poderá ocorrer nos seguintes momentos

- Carga da urna
- Estações de trabalho
- JE Connect
- Comunicação / REDE
- Servidor

6. Pontos de intervenção

- No flash de carregamento, na tentativa de subir um arquivo malicioso
- Nas estações de trabalho que fazem a comunicação com o os servidores do TSE
- Modificar ou/e capturar os dados trafegados pela rede via o JE connec
- Explorar o servidor receptor do TSE
- Tentativas de indisponibilizar os serviços

7. Passos a serem realizados

1) Instação dos sistemas operacionais

2) Instalação e atualização de ferramentas e pacotes dos sistemas operacionais

3) Após a varredura, identificação e mapeamento de toda infraestrutura e com a devida autorização da comissão organizadora, baixar softwares, ferramentas, exploits, frameworks que possam se fazer necessários para exploração.

8. Material necessário

Para execução do teste, será necessário uma máquina capaz de rodar o Kali Linux e virtualização, com as ISO'S do Kali Linux e do Windows 7, 8 ou 10.

Também um dispositivo de armazenamento de pelo menos 60gb, onde serão baixados e armazenados softwares, ferramentas que possam ser úteis no ambiente de teste.

9. Possíveis resultados e impacto

O resultado esperado descrito no plano de teste, é de conseguir explorar os sistemas de proteção da urna eletrônica, com o objetivo de modificar, alterar ou indisponibilizar toda cadeia que envolve os votos.

10. Rastreabilidade

Será possível evidenciar o ataque bem sucedido, através do relatório gerado por mim, onde será possível replicar o ataque pela equipe do TSE e também, através dos logs nas máquinas onde serão executados os testes.

11. Solução proposta

A primeira solução é investir no treinamento dos funcionários e voluntários que de alguma maneira, tem contato com as urnas eletrônicas ou que utilizam a rede do TSE, pois é através do ser humano e o seu comportamento que se encontram as maiores fragilidades em um ataque.

A outra solução é realizar a análise constante dos códigos desenvolvidos pelo TSE, bem como também, de todos os sistemas que envolvem o ambiente da urna eletrônica, buscando as melhores tecnologias, sistemas e protocolos.

Investigador individual – Leonardo Cunha dos Santos

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Teste de invasão utilizando análise instantânea de pulso elétrico

Instituição proponente (se aplicável)

Universidade de São Paulo

Responsável

Leonardo Cunha dos Santos

Resumo do teste (máximo de 120 caracteres)

O teste constitui-se do uso de reconhecimento de padrões a partir da detecção de pulsos elétricos com a finalidade de compreender comportamentos do equipamento durante a operação de voto.

Sistemas afetados

Softwares

(X) *Software Desktop* para preparação de mídia de urna eletrônica
(X) *Software* básico da urna eletrônica
(X) Aplicativos da urna eletrônica
(X) Sistemas de transmissão e recebimento de arquivos de urna eletrônica
(X) Subsistema de Instalação e Segurança (SIS)

Hardwares

(X) Urna eletrônica
(X) Transmissão de arquivos (*Kit* JE Connect)

Procedimentos

(X) Geração de mídias
(X) Carga da urna
(X) Votação
(X) Transmissão de arquivos

DETALHAMENTO DO TESTE

1 – Descrição geral do teste

O teste constitui-se do uso de reconhecimento de padrões a partir da detecção de pulsos elétricos com a finalidade de compreender comportamentos do equipamento durante a operação de voto.

2 – Fundamentação teórica

O teste se baseia no comportamento elétrico do equipamento dispondo de entender a operação como um todo, usando características como consumo energético, tensão, corrente e outras métricas para classificar o voto utilizando estes como parâmetros de entrada.

3 – Precondições para o teste

Com a urna pronta para votação, é preciso conectar na urna elementos capazes de extrair essas métricas.

4 – Escopo – Superfície de ataque

O ataque tem como objetivo descobrir quem votou em quem.

5 – Janela de atuação simulada do atacante

O foco é atuar no processo de confirmação do voto.

6 – Pontos de intervenção

Ainda não foi possível estimar escopo.

7 – Passos a serem realizados

Conectar dispositivos; simular treinos; e testar modelo.

8 – Materiais necessários (fornecidos pelo TSE)

Equipamento pronto para votação e fios que se possam utilizar para ligação

9 – Possíveis resultados e impacto

A quebra do sigilo do voto

10 – Rastreabilidade

É possivel ter um histórico do compotamento do equipamento para a realizacao das operacoes

11 – Solução proposta

Adicionar rotinas que produzam um ruido nas métricas durante essas operações

Protocolo	Data 27/10/2019
	Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Anexo F – Formulários de acompanhamento dos testes públicos

Grupo 1

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Felipe Ribeiro Silva Abib	
Investigador 1 Alan Papafanurakis Heleno	
Investigador 2 Caio Henrique de Aquino	
Investigador 3 Vicente Charles Willian Biesseki	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento		Rubrica	

DADOS DO TESTE	
Título do teste Manipulação do Boletim de Urna	
Início do teste (data/hora)	
Término do teste (data/hora)	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
Para o desempenho das atividades planejadas nos testes a serem executados, foi solicitada a senha de acesso à BIOS dos micros com o objetivo de alterar a ordem de boot do microcomputador da JE.

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Saber como é gerado o BU inicial	
2	Conhecer os dados armazenados	
3	Identificar os eleitores e seus votos	
4	Reconhecer sua criptografia e refazer esse passo em um novo BU modificado pela equipe	
5		
6		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:00	Início dos Trabalhos do dia 25/11/2019.
09:05	Ao se fazer o recebimento dos equipamentos, a equipe de investigadores observou que a leitora flash estava com o serial number diferente daquela descrita na declaração de responsabilidade. Foram feitas anotações no verso da declaração com o serial number correto.
09:15	Equipe copiou programas que estavam no pendrive para o HDD do micro para explorar o BU
09:25	Tentativa de BOOT pelo pendrive nas máquinas com SIS instalado, porém sem sucesso pois a BIOS do micro não estava configurado para BOOT via USB. Solicitado à comissão organizadora a senha de acesso a BIOS.
10:45	Enquanto aguardavam a senha de acesso à BIOS, equipe de investigadores foi até a área de visualização do código-fonte.
11:20	O microcomputador com SIS instalado necessitou reparos e foi trocado pela equipe de apoio. Foi retirado o microcomputador cujo patrimônio é 075.731 e substituído pelo microcomputador 074.187. Conforme informações da equipe que efetuou a troca do micro, devido às alterações na BIOS para a tentativa de BOOT via USB, as configuração de BOOT seguro foram a causa da falha no SIS.
13:33	Retorno às atividades do teste.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
13:48	Foi utilizada uma unidade de DVD-R externa com o SO Kali instalado para dar BOOT no micro com SIS.
14:31	Equipe de investigadores foi até a área de visualização do código-fonte.
15:42	Equipe de investigadores gerou uma mídia de carga e fez a carga da urna.
15:57	Equipe gerou mídia de votação e fez autoteste da urna. Urna pronta para votação.
16:41	Foram selecionados 8 eleitores e fizeram um voto para cada prefeito e vereador, na ordem decrescente da zerézima. Terminada a votação, encerrou a mesma e foi gerado o BU e MR foi retirada.
17:12	Tentativa de verificação do conteúdo dos arquivos gerados na MR, utilizando editores de texto em HEXA decimal.
17:38	Fim dos Trabalhos do dia 25/11/2019.
10:00	Início dos Trabalhos do dia 26/11/2019, chegada do grupo de investigadores.
10:01	Análise do código fonte por alguns integrantes da equipe.
10:02	Utilização de editores Hexadecimal para analisar o conteúdo dos arquivos gerados na MR.
10:03	Análise do arquivo logd. Uso da ferramenta AcessData FX (Editor Hexa).
10:28	Utilização de 7z para tentativa de abertura de arquivos da MR.
10:42	Tentativa de identificação do algoritmo de geração do hash no arquivo de log, ao termino de cada linha do log.
11:09	Geração de urna, nova eleição. Geração de MR de votação.
11:12	Carga na urna.
11:21	Autoteste na urna.
11:43	Alteração da data e hora da urna (ADH).
11:48	Início da votação – urna com poucos eleitores.
11:49	Fechamento da votação.
11:53	Análise dos arquivos gerados na MR.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
12:02	Parada para almoço.
13:49	Retomada dos testes e continuidade da análise dos logs e arquivos gerados na MR. Uso da ferramenta hashcat tentando descobrir o formato do hash.
15:12	Visualização do código fonte.
16:16	Retorno às atividades do teste.
16:34	Tentativa de conversão de Hexa para ASN1. Download da ferramenta.
17:16	Retorno das atividades.
17:17	Leitura do arquivo do RDV utilizando a ferramenta Hexa to Asn.1.
17:32	Equipe conseguiu identificar os votos no RDV.
17:45	Término dos trabalhos do dia 26/11/2019.
09:37	Início dos trabalhos do dia 27/11/2019.
10:10	Faltou o código-fonte das bibliotecas do código fonte do RDV. Equipe técnica disponibilizou o código-fonte das libs para observação da equipe de investigadores.
11:41	Equipe gerou MR de votação.
11:56	Nova votação efetuada.
12:47	Retirada do lacre n. 0286466 da porta USB frontal da máquina patrimônio n. 058.253, para nova cópia do código-fonte das bibliotecas que estavam faltando.
12:48	Verificou-se que a porta USB frontal estava desativada.
12:48	Utilização da porta USB traseira (utilizada inicialmente para o mouse) para cópia do código-fonte faltante.
12:49	Verificou-se que as bibliotecas solicitadas já estavam disponibilizadas na máquina. Não foi feita nova cópia.
12:58	A porta USB frontal foi relacrada com lacre n. 0286478.
13:00	Intervalo de almoço.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
14:11	Retorno do almoço e visualização do código-fonte.
14:15	Atualização do código fonte (rec_arquivos) decrypt/encript das bibliotecas infra. segurança.cepesc.* para versão 1.1.2
14:34	Gerado mídia de votação e autoteste da urna.
15:10	Troca da bobina de papel da urna
15:23	Votação
15:31	Conversão de Hexa para ASN.1 – comparado por o BU do dia anterior, sem nenhuma evidência de encontrar a ordem de votação.
15:40	Gerada nova votação.
15:42	Excluindo ext2 do flash por causa da contra senha.
16:09	Nova votação (utilizando uma seção com menos eleitores para tentar identificar a função aleatória do RDV).
17:48	Fim dos trabalhos do dia 27/11/2019.
09:47	Início dos trabalhos do dia 28/11/2019, chegada dos investigadores.
10:10	Geração da carga da urna.
11:09	Votação e análise do RDV. 1.1- Votar em 1 (um) eleitor por vez. 1.2 Retirar a MR. 1.3 Abrir RDV. 1.4Tentar identificar a posição do voto no RDV. 1.5 Retornar a MR para a urna. 2. Modificar o RDV e enviar o BU para tentativa de identificação da ordem. 3.Retirar a MR antes de finalizar a eleição. 4. Recuperar arquivos anteriores da MR, para a tentativa de identificação da ordem. 5. Abrir o arquivo RDV no formato HEX e tentar identificar o eleitor. 6. Identificação do HASH para verificar conflitos de dados entre o BU e o RDV.
12:21	Intervalo para almoço.
14:32	Retorno do almoço.
14:52	Tentativa de encontrar outros arquivos no flash externo relacionados ao RDV.
18:00	Término dos trabalhos do dia 28/11/2019.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
10:47	Início dos trabalhos do dia 29/11/2019, chegada dos investigadores.
11:02	Geração de um BU e HASH adulterados
11:09	Tentativa de envio dos arquivos adulterados pelo JE-CONNECT
11:32	Preenchimentos dos relatórios finais e finalização dos testes

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim.
As requisições foram atendidas adequadamente?
Sim, foram atendidas, porém com um certo atraso.
O grupo/investigador solicitou algo não contemplado no edital?
Não.
Houve evolução diária no plano proposto?
Sim, porém bem lentamente.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não.
Caso sim, estas alterações foram aprovadas e executadas?

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Ainda não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Não.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES
27/11/2019 Votação realizada para conseguir gerar os arquivos do BU, RDV, IMGBU, JUFA, LOGJEZ, VER e VSCMR para que analisássemos os arquivos com objetivo de identificar a ordem dos candidatos votados para reconstruir a ordem e, assim, identificar os votos de quem votou. Após analisar o BU foi percebido que o RDV está com as matrizes dos candidatos. Agora, estamos vendo o código com o objetivo de prever a aleatoriedade da posição para identificar os votos.
28/11/2019 Na extração dos arquivos que se encontravam na MR, foi encontrado um arquivo deletado com os eleitores que participaram na eleição. Estamos analisando esse arquivo com o RDV para identificar a ordem de rotação no RDV.
29/11/2019 Foi realizada a edição (manipulação) do arquivo RDV e tentado transmitir, porém não foi validado no hás. Tentamos abrir o software RED, mas o arquivo está criptografado.

OBSERVAÇÕES DO GRUPO DE APOIO

O Grupo 1 apresentou um plano de Testes com foco na tentativa de conhecer o processo de geração dos boletins de urnas, tentativa de identificação de padrões, falhas no RDV e identificação da ordem de votação dos eleitores para um determinada seção. Os testes iniciaram com bastante disposição da equipe de investigadores em tentar gerar alguma informação (BU, RDV, etc) por meio da urna eletrônica. Inicialmente, o foco era o BU, mas com desenvolvimento dos trabalhos, a equipe entendeu que os esforços deveriam ser desviados para o RDV. Foram gerados dados de diversas eleições e análises foram executadas com a tentativa de identificação da ordem de votação gravada no RDV. As ferramentas que foram trazidas pela equipe não ajudaram na execução de seus testes. Todas as ações para tentar identificar a ordem de votação foram sem sucesso ou infrutíferas. Por fim, a equipe tentou enviar um BU adulterado utilizando o JE-Connect, mas, também, não logrou êxito. Concluindo, todos da equipe aprenderam bastante sobre os processos envolvidos na votação eletrônica e, certamente, após este TPS, serão bravos defensores da segurança empregada no processo eletrônico brasileiro.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Grupo 2

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Jairo Simão Santana Melo	28/11, 29/11
Investigador 1 Felipe Pradera Resende	25/11, 27/11, 28/11, 29/11
Investigador 2 Leonardo de Almeida Ramos	25/11, 26/11, 27/11, 28/11, 29/11
Investigador 3 Luiz Fernando Sirotheau Serique Junior	Não compareceu
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data 25/11/2019 a 29/11/2019	Hora de início 14:24	Hora de término 16:56	
Responsável pelo acompanhamento	Ralph Werner Gomes Viegas e Dave Pinheiro da Silva	Rubrica	

DADOS DO TESTE	
Título do teste Teste da urna Eletrônica baseado em IA e Processamento de Sinais	
Início do teste (data/hora) 25/11/2019 às 14:24	
Término do teste (data/hora) 29/11/2019 às	
Critério de parada	Quebrar sigilo do voto através da identificação de padrões nos sinais elétricos que trafegam entre o teclado e a placa-mãe da urna eletrônica.

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
Acesso à urna eletrônica sem lacres ou qualquer outro mecanismo de restrição ao hardware. Acesso ao esquemático eletrônico do teclado da urna.

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	A equipe de teste ao recepcionar a urna fornecida pelo TSE, a mesma será aberta coma finalidade de que os sinais [2] de entrada possam ser capturas por um osciloscópio	
2	Após a captura dos sinais produzidos por todas as teclas do teclado, a respectiva coleta será exportada para um arquivo em formato UTF.	
3	Esse arquivo será tratado removendo possíveis interferências	
4	Após a normalização, esse arquivo será submetido a um algoritmo de clusterização [3] escrito em Python [1], buscando identificar a formação de um certo conjunto de família de dados. Essas famílias devem buscar representar sinal de cada tecla do teclado, mesmo que o sinal esteja modulado por uma chave de criptografia a representação de similaridade do sinal retirando a portadora será a mesma.	
5	Será gerado um segundo arquivo, a fim de validar a acurácia gerada no treinamento.	
6	Ao final será gerando um relatório e entregue a instituição.	
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
14:24	Início dos trabalhos do dia 25/11/2019, retirada da urna da caixa.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
14:24	Solicitação de entrada de materiais: 1 osciloscópio Hantek serie 66xx, 1 macbook Pro 2011.
14:28	Urna ligada (carga de treinamento)
14:30	Início do autoteste de urna – versão brigadeiro
14:37	Final do autoteste
14:38	Abertura do gabinete da urna (frontal)
14:44	Cabo do teclado desconectado
14:48	Osciloscópio conectado ao cabo do teclado
14:51	Urna ligada com bateria desconectada
14:52	Urna religada (com impressora conectada)
14:58	Osciloscópio conectado no pino verde (data mais) da USB do teclado
14:59	Urna habilitada para votar
15:00	Início da digitação no terminal do eleitor
15:02	Início da análise utilizando software Pulse View (notebook – MacOs)
15:05	Início da análise utilizando software Open Hantek
15:15	Digitação no terminal do eleitor
15:26	Conexão do osciloscópio ao pino branco (data menos) da USB do teclado
15:30	Digitação no terminal do eleitor
15:34	Gravação análise-referência teclado sem apertar tecla
15:49	Análise da USB da impressora para comparar com o sinal do teclado
16:13	Inserção da MR
16:14	Captura de sinal na USB da MR
16:15	Urna reinicializada
16:21	Análise de sinal da USB da MR

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
16:25	Gravação do sinal das teclas do terminal do eleitor
16:28	Gravação do sinal da tecla 1 (terminal do eleitor)
16:30	Gravação do sinal da tecla 2
16:31	Gravação do sinal da tecla 3
16:32	Gravação do sinal da tecla 4
16:33	Gravação do sinal da tecla 6
16:34	Gravação do sinal da tecla 5
16:35	Gravação do sinal da tecla 7
16:35	Gravação do sinal da tecla 8
16:36	Gravação do sinal da tecla 9
16:36	Gravação do sinal da tecla 0
16:37	Gravação do sinal da tecla “CORRIGE”
16:37	Gravação do sinal da tecla “BRANCO”
16:38	Gravação do sinal da tecla “CONFIRMA”
16:40	Captura da oscilação da USB do microterminal
16:55	Fim dos trabalhos do dia 25/11/2019.
14:35	Início dos trabalhos do dia 26/11/2019.
14:35	Solicitação de entrada de materiais (1 pendrive).
14:40	Instalação de osciloscópio na máquina de apoio Windows.
14:50	Instalação de softwares para uso do osciloscópio na maquina de apoio Windows.
15:12	Consulta ao código-fonte.
17:27	Retorno do ambiente do código-fonte.
17:39	Solicita saída de material. Autorizada a saída do equipamento osciloscópio.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
17:56	Lacração dos equipamentos.
18:00	Fim dos trabalhos do dia 26/11/2019.
14:05	Início dos trabalhos do dia 27/11/2019.
14:05	Solicitação de entrada de material – 1 osciloscópio, 1 pendrive e 1 cabo de áudio P2.
14:21	Montagem do osciloscópio conectando o canal 1 no D- e canal 2 no D+ da USB do teclado.
14:48	Captura de amostras de tensão do teclado sem apertar teclas. Foi utilizado codificador para interpretar sinais de tensão em pacotes USB, mas não foi identificado nenhum padrão aproveitável, embora tenha sido identificado pulsos na frequência de 1 KHz. Nenhum padrão ou estrutura de dados identificado nos pulsos.
14:50	Inserção de cabo de áudio na saída P2 da urna conectando-o ao canal 1 do osciloscópio.
14:52	Tentativa de identificação de sinal no cabo de áudio que pudesse evidenciar acoplamento eletromagnético entre o circuito de áudio o circuito do teclado. Não foi detectada evidência deste acoplamento e detectou-se apenas ruído branco.
17:05	Fim dos trabalhos do dia 27/11/2019.
14:15	Início dos trabalhos do dia 28/11/2019.
14:22	Solicitação de entrada de materiais: 1 osciloscópio, 1 HD externo, 2 fios protoboard.
14:23	Análise visual dos dados das teclas 0-9, Branco, Corrige e Confirma coletados nos arquivos do dia 25/11.
15:37	Concatenação de dois arquivos (das teclas 0 e tecla 1) com dados filtrados (filtro das amostras >2V e !=2.5V). Com a aplicação do filtro, espera-se a eliminação de ruído que possam atrapalhar o algoritmo de aprendizagem.
16:00	Execução de programa python com o arquivo filtrado como entrada, com utilização de biblioteca kmeans, parametrizado para 3 clusters (1 cluster para cada tecla e 1 cluster default), para aprendizagem de dados do arquivo concatenado. O programa retornou três centroides e três labels.
16:18	Concatenação dos treze arquivos (todas as teclas da urna), sem filtro. Arquivo resultante com 1,2GBytes
16:30	Execução de programa python com o arquivo de 1,2 GB (sem filtro) como entrada, com utilização de biblioteca kmeans, parametrizado para 14 clusters (um para cada tecla e um adicional para ruído). O programa “crashou” sem retornar resultado.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
16:32	Aplicação de filtro das amostras !=2.5V no arquivo de 1,2GB, para eliminação de ruído e consequente diminuição do tamanho do arquivo de 1,2Gbytes (motivo pelo qual programa “crashou”).
16:35	Execução de programa python com o arquivo filtrado como entrada, com utilização de biblioteca kmeans, parametrizado para 14 clusters (um para cada tecla e um adicional para default/ruído). O programa retornou quatorze centroides e apenas dois labels.
17:01	Plotagem dos centroides junto à massa de dados em um gráfico X,Y para visualizar e tirar prova da presença de apenas dois labels.
17:50	Finalização dos trabalhos do dia 28/11/2019.
13:20	Início dos trabalhos do dia 29/11/2019.
14:22	Medição e gravação do sinal elétrico do teclado pressionando-se um única tecla repetidas vezes com o objetivo de identificar, dentro os pulsos de 1Khz, aqueles relacionados ao pressionamento da tecla.
14:37	Foi solicitado o esquemático eletrônico do teclado da urna.
15:08	Foi fornecido o esquemático eletrônico do teclado da urna.
15:21	Na ferramenta de captura (pulse view) foi selecionado visualmente e gravado, dentre os pulsos de 1KHz capturados, um pulso de maior duração.
15:22	Na ferramenta de captura (pulse view) foi selecionado visualmente e gravado, dentre os pulsos de 1KHz capturados, um pulso de duração comum (pulso típico).
15:25	Os pulsos colhidos no passo anterior foram plotados em um gráfico XY. Esperava-se a identificação visual de dois grupos de pontos (dois aglomerado de pontos distintos). Entretanto, a distribuição dos pontos foi relativamente dispersa e não foi possível essa identificação.
15:35	Medição e gravação do sinal elétrico do teclado pressionando-se a tecla 7 repetidas vezes com o objetivo de identificar, dentro os pulsos de 1Khz, aqueles relacionados ao pressionamento da tecla.
15:36	Na ferramenta de captura (pulse view) foi selecionado visualmente e gravado, dentre os pulsos de 1KHz capturados, um pulso de duração longo.
15:40	Medição e gravação do sinal elétrico do teclado pressionando-se a tecla 8 repetidas vezes com o objetivo de identificar, dentro os pulsos de 1Khz, aqueles relacionados ao pressionamento da tecla.
15:41	Na ferramenta de captura (pulse view) foi selecionado visualmente e gravado, dentre os pulsos de 1KHz capturados, um pulso de duração longo.
15:46	Medição e gravação do sinal elétrico do teclado pressionando-se a tecla 9 repetidas vezes com o objetivo de identificar, dentro os pulsos de 1Khz, aqueles relacionados ao pressionamento da tecla.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
15:48	Na ferramenta de captura (pulse view) foi selecionado visualmente e gravado, dentre os pulsos de 1KHz capturados, um pulso de duração longo.
16:05	Concatenação de três arquivos (das teclas 7, tecla 8 e tecla 9) com pulsos selecionados visualmente, mas não filtrados.
16:12	Aplicação de filtro das amostras !=2.5V no arquivo concatenado, para eliminação de ruído.
16:35	Execução de programa python com o arquivo filtrado como entrada, com utilização de biblioteca kmeans, parametrizado para 4 clusters (um para cada tecla e um adicional para default/ruído). O programa retornou quatro centroides e quatro labels.
16:56	Finalização dos trabalhos do dia 29/11.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim, o plano foi seguido, porém encontraram dificuldade em isolar o sinal a ser analisado.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim. Ocorreu apenas uma pequena falha intermitente no monitor da máquina de apoio Windows que não chegou a atrapalhar o andamento dos trabalhos.
As requisições foram atendidas adequadamente?
Sim.
O grupo/investigador solicitou algo não contemplado no edital?
Sim, o esquemático eletrônico do teclado da urna.
Houve evolução diária no plano proposto?
Sim. O plano foi seguido, porém parou no ponto em que não foi alcançado o objetivo de identificar padrão para cada tecla. Assim, não foi possível fazer a prova, ou seja, coletar uma sequência de dígitos da urna e identifica-los apenas pelo padrão de sinal elétrico gerado, através da comparação dos padrões das teclas (padrões não identificados).

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não.
Caso sim, estas alterações foram aprovadas e executadas?
-
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Sim. O grupo esperava um nível maior de dificuldade para medir os sinais elétricos do teclado, como um teclado que se conectasse diretamente à placa-mãe por soquete (sem uso de cabos e conectores USB) onde a medição de sinais só pudesse ser feita com a desconexão do teclado.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Não.
O plano de teste proposto pelo grupo de investigadores pressupunha a identificação das teclas da urna através de padrões aprendidos por AM (aprendizagem de máquina) e que poderia ser utilizado para quebrar o sigilo do voto. Entretanto o grupo não foi obteve êxito na classificação (rotulação) dos sinais capturados e no mapeamento dos sinais nas teclas correspondentes da urna. Existia também a intenção de verificar se era possível a captura de sinais do teclado na saída de áudio P2 da urna através de acoplamento eletromagnético dos circuitos de tais periféricos. O grupo não obteve êxito obtendo apenas ruído branco na saída de áudio. É importante relatar que, embora tenha sido utilizado um osciloscópio para medir os sinais elétricos diretamente dos cabos que conectam o teclado à placa-mãe da urna, o houve dificuldade em identificar os padrões de pacotes USB. Este fato criou um obstáculo para o sucesso do processo de separação do ruído e sinais de controle da carga útil do sinal (filtragem do sinal). Sem uma filtragem adequada, tornou-se difícil o aprendizado efetivo do algoritmo de AM. Cabe salientar que o grupo esperava um nível maior de dificuldade para medir os sinais elétricos do teclado, como um teclado que se conectasse diretamente à placa-mãe por soquete (sem uso de cabos e conectores USB) onde a medição de sinais só pudesse ser feita com a desconexão do teclado.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES

Durante a execução dos testes no ambiente controlado do TSE, foi possível realizar algumas coletas de sinais com o osciloscópio Hantek. As coletas buscavam identificar sinais diferenciados de cada tecla, contudo encontramos algumas dificuldades em isolar o sinal.

Mesmo com o dataset contendo ruídos, submetemos os dados ao algoritmo kmeans onde foi possível inicialmente identificar 3 clusters e posteriormente esperava-se 14 clusters.

Neste sentido a arquitetura do teste demonstrou-se viável, entretanto é necessário melhorar o processo de coleta do sinal.

Foi possível captar o sinal de telado sem precisar desconecta-lo ou danificar a urna. Há uma blindagem nas teclas, mas a conexão USB é vunerável. Pode ser instalado um sensor para registrar a abertura da urna.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Grupo 3.1

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Luis Antonio Brasil Kowada	
Investigador 1 Gabriel Cardoso de Carvalho	
Investigador 2 Victor Faria de Sousa	
Investigador 3 Igor Palmieri Antunes OBS.:(Não se apresentou para os testes em nenhum dia)	
Investigador 4 Ramon Rocha Rezende	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento	DILSON ATHIAS MESQUITA (TRE-PA) / LUIZ OTAVIO DUARTE (FACTI)	Rubrica	

DADOS DO TESTE	
Título do teste Tentativa de obtenção de chaves criptográficas.	
Início do teste (data/hora) 25/11/2019 15:43	
Término do teste (data/hora) 26/11/2019 16:50	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
Não Houve

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Análise da alimentação dos dados sobre candidatos, seções e eleitores nos servidores através do sistema GEDAI-UE.	
2	Análise da alimentação dos dados sobre candidatos, seções e eleitores nas urnas através do software de carga SCUE.	
3	Análise da manipulação destas informações pelo GAP, VOTA, RED e SA.	

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
15:43	Início dos trabalhos do dia 25/11/2019.
15:43	Verificação do código-fonte.
15:43	BOOT do Kali Linux, através do pendrive, em uma máquina.
15:49	Acesso ao gerenciamento de disco do Windows.
15:51	Início da instalação do Kali Linux no computador.
16:58	Término da instalação do Kali Linux no computador.
18:00	Encerramento dos trabalhos do dia 25/11/2019.
09:10	Início dos trabalhos do dia 26/11/2019 com a verificação do código-fonte.
09:30	Acesso ao GEDAI e geração de flash de carga.
09:45	Verificação das partições do flash de carga no Kali Linux.
10:09	Atividades em arquivos .JEZ
10:00	Os arquivos .JEZ foram abertos na máquina Linux e os conteúdos foram avaliados.
10:54	Foram realizadas inspeções nos arquivos .VST (VOTA-BU, AVPORT, VOTA-IMG e outros)
11:05	Solicitada a entrada de pendrive com informações e documentos.
14:40	Uso do flash de carga para preparar a urna.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
14:50	Análise dos arquivos (apenas visualização) de diversas pastas do flash de carga (pasta: / MNT/BIN)
15:10	Desassembly AES-SET-DECRYPT-KEY e AES-SET-ENCRYPT-KEY contido na flash de carga.
15:42	Hex Dump do arquivo AVUSRLIB.VST contido no flash de carga.
16:50	Fim dos trabalhos no dia 26/11/2019.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
O grupo de investigadores tentou seguir o plano proposto. Entretanto, aparentemente o plano foi construído sobre o conhecimento que possuíam sobre versões antigas do software da urna, de forma que essa premissa inicial - que era fundamental para a continuidade do plano de teste - acabou por inviabilizar sua progressão da maneira estritamente como foi proposta. Desta forma, o grupo buscou identificar maneiras alternativas de prosseguir no seu plano de testes, sem, entretanto lograr êxito na obtenção de chaves criptográficas ou de vulnerabilidades em bibliotecas.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim a infraestrutura mostrou-se adequada aos propósitos do teste.
As requisições foram atendidas adequadamente?
Sim, todas as requisições de informações técnicas (duas) e de entrada de materiais (três) foram prontamente atendidas.
O grupo/investigador solicitou algo não contemplado no edital?
Não.
Houve evolução diária no plano proposto?
Por conta do que foi relatado anteriormente, os progressos alcançados foram prejudicados, uma vez que a frente de atuação voltou-se a identificação de novos caminhos para obter sucesso nos planos propostos.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não.
Caso sim, estas alterações foram aprovadas e executadas?
Não se aplica

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Uma sugestão seria realizar uma rápida reunião prévia com os investigadores, no primeiro dia, para esclarecer como será o decorrer do TPS, como serão colhidos os formulários, quais são os de preenchimento obrigatório, o que é permitido e o que não é etc.

OBSERVAÇÕES DO GRUPO DE APOIO
O plano apresentado por este grupo de investigadores teve por objetivo verificar controles de segurança presentes nos processos utilizados nos sistemas de software de urna eletrônica. Sobretudo, a proposta, de alguma forma, buscou verificar fragilidades anteriormente já reportadas por outros grupos de investigadores em Testes Públicos de Segurança ocorridos em anos anteriores. Muito por conta das alterações que o Tribunal realizou nos ativos de software, o grupo de investigadores acabou por se ver diante de novos desafios e barreiras que precisariam ser transpostas. Durante a realização de suas atividades tais barreiras não puderam ser contornadas conforme expostas nos planos que os grupos apresentaram.

_____

DILSON ATHIAS MESQUITA
TRE-PA

_____

LUIZ OTAVIO DUARTE
Facti

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES

Sem êxito nos testes elaborados.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

DILSON ATHIAS MESQUITA
TRE-PA

_____

LUIZ OTAVIO DUARTE
Facti

Grupo 3.2

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Luis Antonio Brasil Kowada	
Investigador 1 Gabriel Cardoso de Carvalho	
Investigador 2 Victor Faria de Sousa	
Investigador 3 Igor Palmieri Antunes OBS.:(Não se apresentou para os testes em nenhum dia)	
Investigador 4 Ramon Rocha Rezende	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento	DILSON ATHIAS MESQUITA (TRE-PA) / LUIZ OTAVIO DUARTE (FACTI)	Rubrica	

DADOS DO TESTE	
Título do teste Verificar as vulnerabilidades da biblioteca do sistema.	
Início do teste (data/hora) 27/11/2019 09:20	
Término do teste (data/hora) 29/11/2019 XX:XX	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
Não Houve

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Engenharia reversa no kernel para tentativa de recuperação de chaves criptográficas.	
2	Busca de vulnerabilidades aplicáveis em bibliotecas externas.	
3	Busca de Conteúdo não assinado.	
4	Em caso de existência de conteúdo não assinado e das chaves serem encontradas, haverá tentativa de alteração do código.	

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:20	Início dos trabalhos do dia 27/11/2019.
09:20	Uso da máquina Linux.
09:30	Verificação de arquivos do FC de carga, pastas /etc e /mnt/lib com uso de comandos cat / hexdump/ strings/ grep / ls
09:38	Solicitação de informação técnica acerca do mecanismo de geração de números aleatórios da urna.
10:00	Solicitação de informação técnica sobre o projeto do TRNG.
10:10	Regeração do FC de carga no GEDAI versão TPS.
10:16	Nova verificação dos arquivos da FC de carga regerada. Pasta /lib (libapihwil2006.so)
10:20	Alterado o link do arquivo libapihwilue.so para libapihwil2006.so. Entretanto, após nova carga da urna o próprio procedimento de carga mudou o link para libapihwil2015.so (versão da urna utilizada).
11:00	Alterado o conteúdo do arquivo libapisdkurna2.so, com alteração do link para o arquivo / uenux/lib/libapidsk.so.
11:20	Reinício da urna com nova carga, após as alterações feitas na FC de carga – carga de nova seção (seção 02). Observação: Não apresentou nenhum erro na carga – com emissão do comprovante de carga.
11:25	Geração de mídia de resultado e FV para a urna/ simulado.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
11:40	Como resultado da solicitação de informação técnica feita às 10:00 horas, o servidor Luis Consularo forneceu dados* ao investigador Kowada, através de um pendrive, cópia feita no computador 57.527 na área de internet, rompendo o lacre nº 0286484 que estava na entrada USB, tendo sido feita a relacração com o lacre nº 0286479. (*) dados fornecidos foram: Esquema técnico do terminal do mesário; Esquema técnico do teclado do eleitor; Esquema técnico da CPU; Esquema técnico da impressora; Firmwares em geral das urnas relacionados ao TRNG; Documentações relacionadas aos firmwares fornecidos.
14:00	Reinício dos testes.
14:00	Leitura do material técnico trazido pelos investigadores.
14:40	Inicialização da urna com a FV e MR geradas às 11:25
14:48	Emissão da Zerésima
14:49	Início da Votação Simulada
14:55	Enceramento da Votação
15:01	Nova tentativa de carga com arquivos corrompidos pelos investigadores (AVBOOT.VST). No processo de verificação prévio à carga, a urna eletrônica interrompeu a execução no processo 05/30 – observação: Led Vermelho contínuo no MT.
15:08	Na sequência, os investigadores corromperam o arquivo de BOOT do UENUX contido na flash de carga e a urna retornou , logo nos primeiros segundos de inicialização o erro “Retorno MS0 1XD: assinatura inválida”.
15:20	Solicitação de acesso à flash interna da urna.
15:40	Após autorização, foi feito o acesso à flash interna da urna com o leitor de flash e realizada a cópia de todo o seu conteúdo para uma pasta no computador.
16:25	Os investigadores realizaram análise de arquivos da flash de carga diretório /MNT/LIB e copiaram o conteúdo para outra pasta.
16:41	Geração de nova flash de carga no GEDAI.
17:20	Um outro arquivo da flash de carga foi alterado (arquivo AVUSRLIBUE2010.VST) e a urna travou na verificação da integridade, etapa 16/30, ficando o LED VERMELHO ligado de forma contínua no micro terminal, sem mensagem específica de erro no terminal do eleitor.
17:20	Fim dos trabalhos do dia 27/11/2019.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:30	Início dos trabalhos do dia 28/11/2019.
09:30	Pesquisa na área reservada para acesso à internet.
10:10	O grupo de investigadores decidiu alterar permissão de acesso em algumas pastas da flash interna e externa (comando CHMOD).
10:26	Foi feita ainda a troca de posições entre a flash interna e externa. Os investigadores observaram resposta da urna durante o BOOT (a urna apresentou erro)
10:30	Os investigadores inverteram os cabos USB do teclado e do drive da memória de resultado (MR) conectados na placa mãe. A urna não inicializou.
10:36	Nova geração de flash de carga no GEDAI e a realização de nova carga na urna.
10:45	Os investigadores foram para a área reservada para análise do código-fonte.
11:20	Conectado o cabo da MR na porta USB Livre (H4). Durante o autoteste, no momento de verificação da MR, o processo falhou. Entretanto, não houve qualquer aviso/mensagem ao usuário, apenas o checkbox de validação do teste não foi marcado na tela da urna.
11:25	Conectado o cabo da impressora na porta USB (H4) livre, e o autoteste termina normalmente e sem falhas.
14:40	Mudança de atributos do arquivo LIBPIHWILVE.SO da Flash de carga (mas os investigadores nem chegaram a testar o resultado na urna).
15:10	O investigador, prof. Luis Antonio Kowada, comunicou ao apoio técnico que este seria o último dia de teste para ele próprio e para o investigador Gabriel Carvalho. Comunicou ainda que no dia 29/11 estariam presentes ao TPS os investigadores Victor Faria de Sousa e Ramon Rocha Rezende.
15:50	Foi feita a formatação completa das mídias trazidas pelos investigadores (pendrive 8Gb e 32Gb).
18:00	Fim dos trabalhos do dia 28/11/2019.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
O grupo de investigadores tentou seguir o plano proposto. Entretanto, aparentemente o plano foi construído sobre o conhecimento que possuíam sobre versões antigas do software da urna, de forma que essa premissa inicial - que era fundamental para a continuidade do plano de teste - acabou por inviabilizar sua progressão da maneira estritamente como foi proposta. Desta forma, o grupo buscou identificar maneiras alternativas de prosseguir no seu plano de testes, sem, entretanto lograr êxito na obtenção de chaves criptográficas ou de vulnerabilidades em bibliotecas.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim a infraestrutura mostrou-se adequada aos propósitos do teste.

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
As requisições foram atendidas adequadamente?
Sim, todas as requisições de informações técnicas (duas) e de entrada de materiais (três) foram prontamente atendidas.
O grupo/investigador solicitou algo não contemplado no edital?
Não.
Houve evolução diária no plano proposto?
Por conta do que foi relatado anteriormente, os progressos alcançados foram prejudicados, uma vez que a frente de atuação voltou-se a identificação de novos caminhos para obter sucesso nos planos propostos.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não.
Caso sim, estas alterações foram aprovadas e executadas?
Não se aplica
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Uma sugestão seria realizar uma rápida reunião prévia com os investigadores, no primeiro dia, para esclarecer como será o decorrer do TPS, como serão colhidos os formulários, quais são os de preenchimento obrigatório, o que é permitido e o que não é etc.

OBSERVAÇÕES DO GRUPO DE APOIO
O plano apresentado por este grupo de investigadores teve por objetivo verificar controles de segurança presentes nos processos utilizados nos sistemas de software de urna eletrônica. Sobretudo, a proposta, de alguma forma, buscou verificar fragilidades anteriormente já reportadas por outros grupos de investigadores em Testes Públicos de Segurança ocorridos em anos anteriores. Muito por conta das alterações que o Tribunal realizou nos ativos de software, o grupo de investigadores acabou por se ver diante de novos desafios e barreiras que precisariam ser transpostas. Durante a realização de suas atividades tais barreiras não puderam ser contornadas conforme expostas nos planos que os grupos apresentaram.

DILSON ATHIAS MESQUITA
TRE-PA

LUIZ OTAVIO DUARTE
Facti

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES

Plano de teste 2 - Verificar vulnerabilidades nas bibliotecas do sistema

- Foi instalado o Sistema Operacional KALI em uma das máquinas para propósitos de análise das mídias de carga, votação e resultados. Durante as análises, além de estudo do código fonte, foram feitas inspeções nos binários de algumas bibliotecas (principalmente a “libapicryptoc.so”).

– Foi gerada uma mídia de carga e foi feita uma análise desta mídia. Foram encontrados os arquivos de assinatura “.vst” e a análise desses arquivos foram encontradas dois links não assinados no diretório ‘uenux/lib/’ da midia de carga. As bibliotecas linkadas são ‘libapisdk.so’ e ‘libapihwilue.so’. Como teste alteramos os links de ambos, sendo aceitos pela urna, porém constados serem apenas marcadores de controle. Não ouve impacto nesse teste.

– Testes da cadeia de confiança:

1) BootLoader – UENUX
2) Gerenciador de Aplicativos – UENUX
3) UENUX – MSD

Para testar 1) foi alterado o arquivo encriptado ‘uenux’ no diretório ‘boot/’, para a etapa 2), foi alterado o arquivo de assinatura ‘avboot.vst’ no diretório ‘boot/’. Finalmente, para a etapa 3) foi apagada uma parte do arquivo ‘libapicryptoc.so’ no diretório ‘uenux/lib/’ . A urna respondeu corretamente com mensagens de erro ou travando.

Passo 4 – Troca das conexões USB

Há 4 conectores USB na placa-mãe: H1 a H4

H1) MR – Midia de resultado

H2) teclado TE (Terminal do Eleitor)

H3) MI - Impressão

H4) vazio

Trocando MI para H3 : não há detecção de erro, e a impressora funciona normalmente (imprime).

Trocando teclado TE para H3 : o sistema exibe uma mensagem em loop contínuo, mas trocando o teclado para H2, o sistema continua dando boot e volta a funcionar normalmente

Trocando MR para H3, não há detecção de erro. Porém, no autoteste prévio à votação, o teste da MR falha.

(Continuação)

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES
Obs. Iniciando MI em H3, e posteriormente mudando MI para H4, a impressão continua funcionando. Plano de teste 1 - Tentativa de obtenção de chaves criptográficas - Inspeção do código fonte das bibliotecas criptográficas afim de entender o procedimento e onde as chaves eram utilizadas. - Inspeção do binário da biblioteca 'libapicryptoc.so' contida na mídia de carga. - Observação: Encontrado o diretório de chaves na cache do Eclipse em maquina virtual, no ambiente de codigo fonte.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

DILSON ATHIAS MESQUITA

TRE-PA

_____

LUIZ OTAVIO DUARTE

Facti

Grupo 4

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Luis Fernando de Almeida	
Investigador 1 Fabio Rosindo Daher de Barros	
Investigador 2 Gabriel Ferrari Carvalho	
Investigador 3 Fernando Nogueira da Silva	
Investigador 4 Josinei Rodrigues Lopes Silva	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento		Rubrica	

DADOS DO TESTE	
Título do teste Tentativa de mapeamento de rotina aleatórias por meio de algoritmos de reconhecimento de padrão.	
Início do teste (data/hora)	
Término do teste (data/hora)	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Codificação de algoritmos de Machine Learning (ML) para modelos preditivos.	
2	Simulação de votação utilizando urna eletrônica. 1. Essa simulação será da seguinte forma: primeiro voto para o candidato 1, segundo voto para o candidato 2, até o voto 99, do eleitor 99. Após isso gera o BU da urna. 2. Fazer esta simulação mais de uma vez, inicialmente, 5 vezes.	
3	Analisar código fonte para analisar o procedimento para geração da semente da rotina aleatória.	
4	Submeter o arquivo de dados para os algoritmos para verificar a possibilidade de se criar o modelo da rotina aleatória.	
5	Obtido sucesso, executar nova simulação em paralelo com o programa para verificar se é possível predizer a posição de gravação de cada voto.	
6		
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
:	Investigadores não compareceram no dia 25/11/2019.
09:20	Início dos trabalhos do dia 26/11/2019.
09:38	Solicitação de informações técnicas.
09:39	Instalação da ferramenta Phyton – Windows 10.
09:49	Geração de flash de carga.
09:59	Geração de flash de carga de duas – seções 002 e 003
10:04	Início da carga na urna.
10:24	Nova geração de flash de votação – seções 539 e 568
10:34	Carga na urna – seção 539
10:44	Carga na urna – seção 568
10:53	Início da votação na urna – seção 539.
11:00	Início da votação na urna – seção 568.
11:03	Fim da votação na urna– seção 539. Foram realizadas 20 votações.
11:04	Fim da votação na urna – seção 568. Foram realizadas 10 votações.
11:04	Atividades dos investigadores na tentativa de leitura da flash de votação – seção 539. Falha: não conseguiram o acesso.
11:10	Leitura da flash votação - seção 539 – Linux
11:14	Analisando arquivo RDV. Bloqueio na tentativa de leitura – arquivos criptografados.
11:37	Leitura da flash de votação – seção 568. Bloqueio na tentativa de leitura – arquivos criptografados.
11:55	Encerramento da votação seção 539.
11:57	Encerramento da votação – seção 568
12:05	Análise dos arquivos da mídia de resultado usando o Debian (RDV)
12:21	Intervalo de almoço
13:49	Leitura das duas mídias de resultado em computador Windows para fins de comparação.
14:18	Instalação do Phyton 3.7

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
14:19	Nova carga nas duas urnas de seção
14:33	Solicitação para impressão da lista de eleitores das seções 539 e 568 da zona 039 do município de Palmas.
14:48	Retirada do lacre n. 0286487 de acesso à porta USB da máquina com acesso a internet para cópia de alguns executáveis. Autorizado pela Comissão Reguladora. Arquivos: Numpy, Pycrypto, Scipylearning, Kali.
14:50	Início da votação na urna de seção 568.
15:00	Início da votação na urna de seção 539.
15:31	Colocação de novos lacres nas portas USB do computador com acesso a internet.
15:42	Encerramento da seção 539
15:43	Encerramento da seção 568.
15:55	Instalação do Phython
16:11	Desenvolvimento de algoritmos em C++ e Phython para visualização de conteúdo do arquivo RDV contido na MR.
17:30	Solicitação de arquivo contendo a estrutura do arquivo RDV.
18:00	Lacração das mídias e ferramentas.
18:00	Fim dos trabalhos do dia 26/11/2019.
09:05	Início dos trabalhos do dia 27/11/2019.
09:10	Continuação dos trabalhos do dia anterior de tentativa de visualização do conteúdo do RDV da MR. Algoritmos em C++ e Phyton. Tentativa de transformação do arquivo binário para Hexadecimal
10:45	Com os arquivo RDV gerados pela MR em claro (decifrado), foram feitas análises para verificar as posições de armazenamento dos votos no arquivo. Início da investigação da regra/padrão aleatória de distribuição dos votos no RDV (método de redes neurais).
11:00	Carga da seção 001 (17 eleitores).
11:15	Geração de contra senha para liberar a carga.
11:33	Início da votação – seção 046
11:41	Fim da votação – seção 046 (urna encerrada).
12:06	Intervalo de almoço.
13:31	Retorno do almoço.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
15:02	Nova carga de urna eletrônica – seções 539 e 568
15:18	Início da votação.
15:20	Início da programação (c++) da rede neural que tentará quebrar o padrão de distribuição dos votos no RDV.
16:16	Carga da seção 529, zona 029, município de Palmas.
16:20	Carga da seção 537, zona 029, município de Palmas.
16:22	Início da votação da seção 529.
16:25	Início da votação da seção 537.
17:10	Fim da votação da seção 529.
17:30	Desligamento da urna da seção 537.
17:50	Fim dos trabalhos do dia 27/11/2019.
09:10	Início dos trabalhos do dia 28/11/2019.
09:15	Codificação de rotina que tenta reproduzir a distribuição aleatória do RDV, com base no que foi entendido do código fonte.
09:50	Início de mais uma votação.
10:26	Consulta ao código e explanação técnica.
12:16	Intervalo para o almoço.
13:50	Retorno do almoço.
14:10	Início de mais uma votação com votação simulando a falta de 1 (um) digito.
14:25	Fim da votação.
14:55	Nova carga.
17:00	Testes nos algoritmos com votações iguais, seções iguais, em duas urnas.
18:00	Fim dos trabalhos do dia 28/11/2019.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim.
As requisições foram atendidas adequadamente?
Sim. É um dos pontos autos da execução dos testes. A presteza, agilidade, disponibilidade apresentada pela a Equipe Reguladora e unidades da STI (TSE) no atendimento a solicitações de informações técnicas, equipamentos, dispositivos, instalações e procedimentos apresentadas pela equipe de investigadores.
O grupo/investigador solicitou algo não contemplado no edital?
Não.
Houve evolução diária no plano proposto?
Sim.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não.
Caso sim, estas alterações foram aprovadas e executadas?
(não se aplica)
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não. Os investigadores não conseguiram transpor ou sequer ameaçar qualquer barreira existente no escopo do ataque, o que sugere efetividade dos mecanismos presentes na parte do sistema a que eles se dedicaram.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
A equipe de investigadores é composta por professor universitário e alunos de cursos de tecnologia. Essa parece ser uma comunidade de grande potencial para se buscar qualificação dos grupos de investigadores associada com a atmosfera de parceria, cooperação, fundamental para os propósitos do TPS e praticamente orgânica, natural da relação da comunidade acadêmica com parceiros e clientes.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Grupo 5.1

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Paulo César Herrmann Wanner	
Investigador 1 Ivo de Carvalho Peixinho	
Investigador 2 Galileu Batista de Sousa	
Investigador 3	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento	Luiz Angelo Daros de Luca Luiz Gustavo Marques Florindo	Rubrica	

DADOS DO TESTE	
Título do teste Extração do conteúdo do disco criptografado do SIS.	
Início do teste (data/hora)	
Término do teste (data/hora)	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Inicialização com LIVE CD para cópia do disco cifrado e dump do registry do Windows para mídia removível.	
2	Caso o primeiro passo não seja possível ler o disco diretamente via interface USB.	
3	Montagem do disco cifrado usando as informações do registro do Windows e o programa Truecrypt.	
4	Caso o não seja possível montar o disco, realizar cópia e inicialização em uma máquina virtual para fazer dump de memória.	
5	Análise e extração da chave em memória com as ferramentas apropriadas.	
6	Montagem do disco cifrado e cópia dos arquivos sensíveis.	
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
10:00	Conferência dos equipamentos.
10:05	Início dos trabalhos no dia 25/11/2019.
10:10	Instalação dos softwares no Ubuntu e no Windows 10: VirtualBox, BurgSuite, Volatility, Busybox e X64dbg.
10:18	Reboot micro - erro sistema operacional.
10:24	Chegada o investigador Peixinho.
10:34	Leitura do código-fonte.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
12:00	Boot com o Sistema Operacional Kali Live e dump do disco rígido (HD).
12:00	Fim dos trabalhos para o almoço.
13:39	Reinício dos trabalhos.
13:39	Abortado o dump do disco rídigo (HD).
13:40	Solicitação da senha da BIOS. A solicitação foi atendida pela equipe de apoio.
13:50	Dump do disco rígido (HD), utilizando VBox, raw ◘ vdi
13:58	Cópia para o pendrive dos arquivos do registro e de arquivos contidos no D:\ como Aplic, SE.hsh (“class-id {4B99CC6BB04A4620-AE4F-BE6139E4275E}”) e SE.pzm
15:12	Desenvolvido um programa para regerar a senha do disco cifrado a partir dos fontes e do arquivo SE.hsh. Sem sucesso.
16:19	Nova tentativa após reanálise dos códigos e alterações do programa desenvolvido. Sem sucesso.
17:40	Término do dump do disco rígido (HD) da máquina SIS.
18:00	Fim dos trabalhos do dia 25/11/2019. A equipe de investigadores dispensou a lacração dos equipamentos.
09:30	Início dos trabalhos do dia 26/11/2019.
09:40	Solicitação de equipamentos.
09:50	Execução da VM com SIS
09:50	Vboxmanage debugvm GEDAI dumpvmcore –filename <nome_do_arquivo>.
:	Inicialização do Hxd (editor hexadecimal)
:	Busca por palavra chave: “truecrypt”, “sisvol”, “sis” e “sus”, sem sucesso na localização da chave
09:51	Instalação do Volatility.
10:00	“volatility –f *.imp truecryptmaster”, sem sucesso na localização da chave
10:04	“volatility –profile –h” , sem sucesso na localização da chave
10:05	“volatility -f dump.imp –-profile=Windows” , sem sucesso na localização da chave
10:05	“volatility –v –d -f dump.imp –profile=Windows” , sem sucesso na localização da chave
10:10	“truecrypt -–force master” , sem sucesso na localização da chave

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
	“truecrypt -f *.imp vboxinfo” , sem sucesso na localização da chave
	“truecrypt -f *.imp truecrypt summary” , sem sucesso na localização da chave
	“virtualbox core dump elf64” , sem sucesso na localização da chave
	Uso do profile Windows10x64 no volatility
	“truecrypt -f imp –profile=win10x64 -10586 p_list” , sem sucesso na localização da chave
	Buscar no dump da memória da VM SIS usando o Hxd por “4692” ou “4692CB”. Sequência de 32bytes em Hexa, sem sucesso na localização da chave
	Buscar no dump da memória da VM SIS usando o Hxd por “D4 D2 2A D9 EB” (string presente no código-fonte que gera a chave). Foi possível localizar a chave 85674244B84A3A-35D247B4FC...
10:33	Montagem do disco cifrado usando a chave localizada
18:00	Término dos trabalhos do dia 26/11/2019.
09:20	Abertura do dia 27/11/2019
12:10	Saída para almoço
13:38	Retorno do almoço.
17:53	Encerramento das atividades do dia 27/11/2019
09:20	Abertura 28/11/2019
18:00	Encerramento das atividades do dia 28/11/2019 (sem atividades nesta linha)
09:10	Abertura 29/11/2019
16:30	Encerramento das atividades do dia 29/11/2019 (sem atividades nesta linha)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim
A infraestrutura solicitada/disponibilizada foi adequada?
Sim

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
As requisições foram atendidas adequadamente?
Sim
O grupo/investigador solicitou algo não contemplado no edital?
Não
Houve evolução diária no plano proposto?
Sim
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não
Caso sim, estas alterações foram aprovadas e executadas?

Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Sim. Foi obtido a chave que cifra o disco M: onde está instalado o GEDAI.
Todavia, o plano não tinha o objetivo de atingir os alvos determinados pelo edital (sigilo e integridade do voto). Ele é requisito para a execução do plano de ataque ao GEDAI.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não deveria ser utilizado como chave um valor que está ou pode ser gerado apenas com as informações presentes na máquina local.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Não.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES (*)
1 – Imagem forense do computador GEDAI/SIS.
2 – Inicialização da imagem em uma máquina virtual.
3 – Dump da memória e busca por strings do SIS para decifrar o volume TrueCrypt na chave encontrada.
4 – Retirada as proteções do SIS para uso do GEDAI.

(*) Documento assinado com as observações do grupo de investigadores segue anexo a este documento.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Grupo 5.2

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Paulo César Herrmann Wanner	
Investigador 1 Ivo de Carvalho Peixinho	
Investigador 2 Galileu Batista de Sousa	
Investigador 3	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento	Luiz Angelo Daros de Luca Luiz Gustavo Marques Florindo	Rubrica	

DADOS DO TESTE	
Título do teste Instalação e execução de código arbitrário em uma máquina do GEDAI.	
Início do teste (data/hora)	
Término do teste (data/hora)	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Inicialização da máquina do GEDAI com LIVE CD para geração da imagem do disco para a mídia removível;	
2	Inicialização da máquina do GEDAI com LIVE CD para geração da imagem do disco para a mídia removível;	
3	Alterações no Registry do disco do GEDAI usando as ferramentas do HIREN´s, com objetivo de suplantar a carga do SIS durante do boot pela imagem principal do GEDAI;	
4	Boot sem SIS na imagem principal do GEDAI;	
5	Alteração de aplicações que geram dados para a urna eletrônica;	
6	Verificação de implantação de dados falsos na Urna Eletrônica.	
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:20	Início das atividades do dia 26/11/2019.
10:00	Abertura corresp_reserva com SQLite
:	Uso do Exeinfo – ver versão e informações GEDAI gedai_ue_exe
:	X64dbg
:	Executou gedai_ue_exe
:	Verificou aspectos e características

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
:	Tentou executar GEDAI
:	Fez testes no GEDAI
:	ProcessMonitor AlterbyGEDAI
:	Estrutura de diretório e exes na register
:	Atenção a not found name
10:20	Chegada da máquina win10 (Solicitação de HW 1).
11:00	Coleta das DLL do sis para rodar o GEDAI fora do SIS.
11:50	GEDAI na VM não tem seções importadas. Solicitado configuração.
12:15	Saída para almoço.
13:50	Retorno do almoço.
14:00	AAAA inseridas com registry editor do Hiren em chaves credential manager
:	ExcludedPro - de Processos
:	X64dbg
:	Busca por UF
:	Disassembly sem sucesso
15:22	Importados dados de seções eleitorais no GDEAI (VM).
15:30	Cópia dos arquivos decriptografados para máquina virtual com SIS.
:	Execução do GEDAI com sucesso.
:	Importados dados de seções eleitorais no GEDAI – SIS com VirtualBox.
18:00	Encerrou as atividades do dia 26/11/2019.
09:20	Abertura do dia 27/11/2019
10:00	HxD S08256TO73440-CA.DAT –Ca dat
	Deletou assinaturas dos arquivos .dat
	Alterou o número do candidato utilizando SQLITE, aberto o banco Gedai-ue.db

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
	Num_processo Eleitoral modificado: 6843
	Insert “alterado” incluído na string Teste Público de Segurança
	Inserção de driver de leitora de cartão no OracleVirtualBox
	Cópia dos volumes disks alterados a serem utilizados na geração das mídias adulteradas.
14:00	Geração de mídia sem arquivo SVC – Erro no GEDAI
	Testes.
	Alterou SO8256TO73440_CA.DAT
	CANDIDATO PREF66/
	Apagou SO8256TO73440-CA.DAT.USC.
	Gedai checa a assinatura e não gera a flash com o arquivo SO8256TO73440_CA.DAT adulterado.
	Chave SECEDITtrava o permissionamento do SECEdit.
	Edição dos usuários do gerenciador de usuários do SIS – A todos os usuários foi atribuído o privilégio de Administrador do micro.
	Filtro de executáveis do SIS Aberto.
	Editadas as chaves: HKLM/Software/Microsoft/Windows/autentication/CredentialProviders com o objetivo de desabilitar a inicialização do SIS.
	Sisexec –A %1 %* Autoriza qualquer programa a executar no SIS. Poderia ignorar hashes e assinaturas.
	Inicialização do Hiren Boot CD 15.2.
	Aberto o Registry Editor PE-Clone utilizando o clone do SIS.
	Com o Registry Editor PE-Clone feita a Busca por Authenticat
	Com o Registry Editor PE-Clone feita a NTFS Access do Hiren – Reescreve NTFS permissões de sistemas eleitorais.
	Com o Registry Editor PE-Clone feita a CISCP pesquisado no sistema operacional.
	Autoruns – Hiren – Pesquisa pelo que é inicializado automaticamente.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
	Busca por SISCP no Hiren Boot.
	Inserção de AAAA nos achados.
	AAAA em sisla.dll.
	Busca por EXCLUDED no Hiren
	NTPW Edit – Trocar senha SAM.
	Todos os passwords alterados para 1 a 8.
	Inicializa SIS no VirtualBox.
	Boot com usuário administrador senha 1 a 8.
09:20	Abertura 28/11/2019
09:20	Ntfsfix /dev/sda1 – aparentemente GEDAI está corrompido.
11:13	Gedai rodou independentemente do SIS quando sisapi.dll foi inserido no mesmo diretório.
	Pacotes adicionais foram instalado, não se sabe se por remoção do protfxp ou por outras alterações no micro virtualizado. Foram feitas várias modificações ao mesmo tempo,
	Protfpxp.sys – remoção protege filesystem
	BasInst – possui muitos logs e muitos detalhes.
	Vboxmanage debugvm SISU(nome dado a vm no virtualBox) dumpvcore –filename –c\imgs\gedai-copiando-media.mem
	Vboxmanage debugvm SISU(nome dado a vm no virtualBox) dumpvcore –filename -c:\imgs\gedai-copia-media-concluida-ok.mem
13:40	Abriu Gedai no DetectiteEasy
	Abriu Gedai no NoVirusThanks
16:39	Solicitação de informação
	Registro: chave de memória encontrada: 85674244B8A34A35D24
16:59	Descoberta! A chave utilizada para cifrar o GEDAI seria composta por um XOR entre “TSE – STI/CSELE/SEVIN e o conteúdo do arquivo chaveiro.pr
	Entrou com XOR-TSE-STI/CSELE/SEVIN e conteúdo chaveiro.pr.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
	A CHAVE COMPOSTA por 48 bytes, sendo: 16 bytes – vetor de inicialização 32 bytes – chave
16:59	Solicitação do binário para abertura do arquivo criptografado que contém a chave de assinatura utilizada pelo GEDAI, indeferida pela Comissão de Organização.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim.
As requisições foram atendidas adequadamente?
Sim.
O grupo/investigador solicitou algo não contemplado no edital?
Não.
Houve evolução diária no plano proposto?
Sim.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não
Caso sim, estas alterações foram aprovadas e executadas?
Não se aplica.
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Sim
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Não.
SUGERIMOS QUE, PARA REPRODUÇÃO DOS TESTES DOCUMENTADOS NESTE FORMULÁRIO, SEJAM PRESERVADAS AS EVIDÊNCIAS DIGITAIS, QUAIS SEJAM: DISCOS RÍGIDOS UTILIZADOS PELOS INVESTIGADORES OU QUE SEJA REALIZADA CÓPIA BIT A BIT DOS COMPUTADORES

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES (*)
1 – Descompactação do GEDAI e retirada da verificação do executável pelo GEDAI.
2 – Alteração do GEDAI para alterar “Local” de votação.
3 – Foi também realizada a decriptação das chaves utilizadas (privadas) pelo GEDAI no debug do GEDAI.

(*) Documento assinado com as observações do grupo de investigadores segue anexo a este documento.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Grupo 5.3

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Paulo César Herrmann Wanner	
Investigador 1 Ivo de Carvalho Peixinho	
Investigador 2 Galileu Batista de Sousa	
Investigador 3	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data	Hora de início	Hora de término	
Responsável pelo acompanhamento	Luiz Angelo Daros de Luca Luiz Gustavo Marques Florindo	Rubrica	

DADOS DO TESTE	
Título do teste Extração de dados e configuração do Kit JE Connect	
Início do teste (data/hora)	
Término do teste (data/hora)	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Realizar imagem da mídia JE Connect	
2	Inicialização a mídia JE Connect em um ambiente virtualizado para realizar um dump de memória	
3	Montagem dos dados existente no sistema de arquivos a fim de identificar credenciais e configuração da VPN	
4	Caso seja possível obter tais informações, estabelecer uma conexão via VPN e testar o recebimento de arquivos utilizando técnicas fuzzing	
5		
6		
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:20	Início das atividades do dia 26/11/2019.
09:40	Solicitação de informação nº 1.
10:08	Troca do Kit JEConnect (Falha no PIN).
10:40	Resposta da solicitação de informação nº 1.
12:15	Saída para almoço.
13:50	Retorno do almoço.
13:50	Feito imagem do JEConnect.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
17:22	Tentativa de executar o JEConnect na VM VirtualBox sem sucesso.
17:40	Tentativa de executar o JEConnect na VM GEMU sem sucesso.
17:56	Encerradas as atividades do dia 26/11/2019
09:00	Início das atividades do dia 27/11/2019.
09:00	Discussão sobre a estratégia JEConnect.
10:08	Cópia de diretórios EFI, Aplic.
17:53	Encerramento das atividades do dia 27/11/2019
09:20	Abertura 28/11/2019
18:00	Encerramento das atividades do dia 28/11/2019 (sem atividades nesta linha)
09:10	Abertura 29/11/2019
16:30	Encerramento das atividades do dia 29/11/2019 (sem atividades nesta linha)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim
A infraestrutura solicitada/disponibilizada foi adequada?
Sim. Os trabalhos foram adiados por falta das mídias do JEConnect. Porém, não prejudicou a equipe que trabalhou nas outras frentes enquanto aguardava a geração das mídias.
As requisições foram atendidas adequadamente?
Sim
O grupo/investigador solicitou algo não contemplado no edital?
Não
Houve evolução diária no plano proposto?
Não. A equipe optou por não solicitar a senha (PIN) do JEConnect. Esta linha de pesquisa não evoluiu além da análise exploratória. A equipe optou por investir os esforços no ataque ao GEDAI.

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não
Caso sim, estas alterações foram aprovadas e executadas?

Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Deve-se preparar o ambiente e executar as rotinas a serem testadas antes do início do TPS.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES
Sem observações dos investigadores, pois esta linha de pesquisa não evoluiu.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Investigador individual – José Filippe de Moraes Albano

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador José Felippe de Moraes Albano	
Investigador 1	
Investigador 2	
Investigador 3	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data: 25/11/2019	Hora de início:	Hora de término:	
Responsável pelo acompanhamento		Rubrica	

DADOS DO TESTE	
Título do teste Exploração de vulnerabilidades na infraestrutura de rede, sistemas e ativos.	
Início do teste (data/hora):	
Término do teste (data/hora):	
Critério de parada	

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
Fornecimento dos PIN´s para os Kit JE-Connect 6843.002.00008 e 6843.002.00018

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
10:55	Início dos trabalhos do dia 25/11/2019.
10:58	Conferência de hardware.
11:18	Solicitação de entrada de materiais nº 01.
11:28	Máquina Windows: carregamento da VM KALI Linux.
12:00	Conexão da máquina Windows com a máquina SIS através de cabo cross.
12:07	Identificação das propriedades de rede da máquina SIS.
12:09	VM Kali Linux: execução do comando nmap –sS –sV <IPMAQSIS> -- system –dns.
12:11	Parada para almoço.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
13:33	Volta do almoço.
13:34	VM KALI Linux: Inicialização do framework Metaexploit.
13:35	Shell do Metaexploit: db_nmap <IPMAQSIS>.
13:40	Shell do Metaexploit: Tentativa de explorar vulnerabilidade de remote desktop (CVE_2019_0708_bluekeep) na porta 3389, sem êxito.
13:48	Shell do Metaexploit: Tentativa de explorar vulnerabilidade de SMB (MS_17_010_PSEXEC) utilizando usuários AVANCADO e ADMINISTRATOR, sem êxito.
13:53	Shell do Metaexploit: Tentativa de explorar vulnerabilidade de execução remota (PEXEC_loggedin-user), sem êxito.
13:54	Shell do Metaexploit: dB_nmap.
14:00	Solicitou entrada de material – 2x HD externos, 2x cabos USB, 1 chave Philips.
14:07	Necessitou de pacote que não existia na VM, reiniciou a maquina Windows, carregando KALI Linux de um HD externo.
14:13	Inicialização do NESSUS pelo navegador (porta 8834), não encontrou a máquina SIS.
14:27	Pesquisa na Internet.
14:32	Reboot da máquina Windows carregando KALI LINUX de um HD externo, não encontrou máquina SIS.
14:44	Máquina Windows: carregamento da VM KALI Linux.
14:51	Máquina SIS: Tentativa de instalação do dumpit, sem êxito.
15:12	Instalação da 3ª maquina para teste do JE-Connect.
15:12	Execução do Kali Linux a partir do HD Externo na máquina sem SIS.
15:15	Instalação do micro para execução de JE-Connect (micro conectado rede).
15:26	Execução de nmap em todas as portas 1 – 65535 (parâmetro –o -A –sV) .
15:40	Execução de msfconsole.
15:58	Execução de nmap em todas as portas 1 – 65535 (parâmetro -T4 --system-dns).
15:58	Execução de msfconsole.
16:01	Investigador utiliza o 3º computador para execução do kit JE-Connect
17:50	Feita a lacração dos materiais.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
17:54	Término dos trabalhos do dia 25/11/2019.
09:15	Início dos trabalhos do dia 26/11/2019.
09:17	BOOT do Kali Linux pelo CD em uma máquina Windows.
09:50	Interligou as estações SIS e Windows10
09:50	Executou o comando netdiscovery no Kali Linux.
09:52	Executou o Nessus (localhost).
09:53	Executou metasploit
09:56	Executou nmap
10:01	No Nessus executou scan para a estação com SIS.
10:10	Nessus apontou vulnerabilidade do SAMBA.
10:11	Tentativa de explorar vulnerabilidade de protocolo SMD via metasploit.
10:28	Executou apache no Kali Linux e habilitou o sniffer.
10:30	Abriu o navegador na máquina com SIS e apontou a URL para a máquina do Kali Linux.
10:39	Acessou o BEEF no Kali Linux.
10:43	Importou base do Nessus para o Metaexploit.
10:45	Investigador desistiu de explorar vulnerabilidade na estação SIS.
10:47	Conectou a estação com Kali Linux na VLAN no ambiente de teste.
11:55	Investigador foi verificar o código-fonte da urna eletrônica e do JEConnect.
12:55	Interrupção para o almoço.
14:02	Executou o nmap da máquina com Kali Linux para o computador do JEConnect.
14:13	Executou o SPARTA visando escanear as portas do JEConnect.
14:31	Executou o Nessus no Kali Linux apontando para o JEConnect.
14:45	Executou o nmap pelo metasploit.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
16:40	Término dos trabalhos do dia 26/11/2019.
10:31	Início dos trabalhos do dia 27/11/2019.
10:58	Execução do nmap no KALI Linux apontando para o micro do JEConnect.
10:59	Execução do ETTERCAP no KALI Linux apontando para o micro do JEConnect e firewall do JEConnect (arp poinsoning).
11:02	Conexão do JEConnect (tentativa de fechamento da VPN).
11:12	Geração da flash de carga.
11:18	Geração da flash de votação.
11:36	Carga da Urna Eletrônica.
11:54	Recarga da Urna Eletrônica, porém investigador conectou teclado na interface USB da Urna Eletrônica para tentar realizar alguma intervenção no processo de boot. Não obteve sucesso.
12:35	Parada para o almoço.
13:38	Retorno do almoço.
13:40	Análise da captura de pacotes de Ettercap: Foram coletados aproximadamente 1MB de dados na captura.
13:53	Impressão da Zeréssima.
13:56	Votação.
14:00	Encerramento da votação.
14:06	Leitura da FC no GEDAI para coleta da tabela de correspondência.
17:08	Transmissão do boletim de urna.
17:09	Ettercap não captura boletim de urna.
17:09	Wireshark não capturou boletim de urna.
18:21	Término dos trabalhos do dia 27/11/2019.
13:36	Início dos trabalhos do dia 28/11/2019.
13:42	Execução de nmap apontando para o cliente do JEConnect.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
13:50	Execução do Ettercap para captura de pacotes do cliente JEConnect e firewall do JE-Connect com arp poisoning habilitado.
14:01	Execução do Wireshark no KALI Linux.
14:02	Conexão do JEConnect.
15:38	Execução do Ettercap apontando para estação de trabalho com SIS. Objetivo: captura de pacotes de GEDAI.
15:49	Ettercap configurado para realizar dns spoofing na estação com SIS.
16:10	Os pacotes capturados não apresentaram dados significativos.
18:00	Término dos trabalhos do dia 28/11/2019.
09:06	Início dos trabalhos do dia 29/11/2019.
09:14	Utilização do dnschef do KALI Linux para a realização de dns spoofing na estação de trabalho com SIS.
09:22	Execução do arp poisoning no Ettercap do KALI Linux apontando para a estação de trabalho com SIS.
09:30	Investigador não obteve êxito na execução dos procedimentos.
09:35	Conexão do equipamento com o KALI Linux com a estação de trabalho com SIS utilizando um cabo crossover.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim.
A infraestrutura solicitada/disponibilizada foi adequada?
Sim.
As requisições foram atendidas adequadamente?
Sim.
O grupo/investigador solicitou algo não contemplado no edital?
Sim. O investigador solicitou realizar análise do Transportador no SIS.

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
Houve evolução diária no plano proposto?
Sim.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Sim.
Caso sim, estas alterações foram aprovadas e executadas?
A solicitação foi negado pois o pedido estava fora do escopo do edital.
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Sim. O investigador solicitou que fosse incluído o sistema Transportador do SIS no escopo do Teste Público de Segurança.

OBSERVAÇÕES DO GRUPO DE APOIO
A proposta do investigador foi realizar exploração de vulnerabilidades na infraestrutura e ativos da Justiça Eleitoral, buscando simular ataques à solução JE-Connect, Urna Eletrônica, GEDAI e estação de trabalho com SIS. O investigador utilizou a distribuição KALI Linux como plataforma para as ferramentas de análise e ataque. Foram utilizados o Metaexploit, Nessus, Ettercap, Wireshark, Beef, Sparta e nmap para vasculhar a infraestrutura, análise de pacotes, verificação de vulnerabilidades, realização de ataques do tipo arp *poisoning* e dns *spoofing* e *man-in-the-middle*. Cabe ressaltar que, a pedido do investigador, foi fornecido o PIN da solução JE-Connect, ação considerada um relaxamento no processo. Os pacotes capturados não apresentaram informações sensíveis de forma a comprometer o sigilo e a integridade dos votos, bem com a infraestrutura disponibilizada para a realização dos testes. As ferramentas de análise de vulnerabilidades não apontaram indícios de brechas que puderam ser exploradas de forma a comprometer a infraestrutura da estação de trabalho com SIS ou da solução JE-Connect. O investigador seguiu seu planejamento proposto inicialmente, porém manifestou o desejo de realizar análise no sistema Transportador do SIS. Sou solicitação não pode ser atendida pois o objeto de análise faz parte do escopo do ambiente do Teste Público de Segurança.

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Investigador individual – Leonardo Cunha dos Santos

DADOS DO GRUPO DE INVESTIGADORES	
Nome	**Freq.**
Investigador coordenador Leonardo Cunha dos Santos	
Investigador 1	
Investigador 2	
Investigador 3	
Investigador 4	

INFORMAÇÕES DO ACOMPANHAMENTO			
Data 26 a 27 de Novembro de 2019	Hora de início 9:30	Hora de término 17:50	
Responsável pelo acompanhamento		Rubrica	

DADOS DO TESTE	
Título do teste Teste de Invasão utilizando análise instantânea de pulso elétrico.	
Início do teste (data/hora) 26/11/2019 – 9:30	
Término do teste (data/hora) 26/11/2019 – 17:50	
Critério de parada	Identificação da destinação do voto (quebra do sigilo do voto)

RELAXAMENTO NOS MECANISMOS E PROCEDIMENTOS DE SEGURANÇA
- A Urna Eletrônica foi fisicamente aberta (necessidade de rompimento dos lacres em campo)
- O investigador teve acesso ao código-fonte e esquema elétrico (informações de acesso restrito)

ETAPAS PROPOSTAS PARA O TESTE		
Etapa	**Descrição**	***Status***
1	Conectar dispositivos.	ok
2	Capturar sinais elétricos durante uma votação	ok
3	Utilizar métodos de inteligência artificial para identificar padrões que possam identificar a destinação do voto (quebra de sigilo)	Sem sucesso
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
09:40	Início dos trabalhos do dia 26/11/2019.
09:40	Solicitação de uma chave Philips.
09:45	Inspecionando código-fonte.
10:10	Abriu a urna.
10:30	Retirou teclado, verificou que é blindado.
11:00	Acoplando Arduino para monitorar correntes na urna.
11:43	Entregue esquema elétrico do teclado.

(Continuação)

ACOMPANHAMENTO DOS FATOS	
Hora	**Fato**
12:15	Almoço
13:15	Reinício. Solicitou informação sobre o teclado ao Rafael.
16:00	Colocou sensores de corrente entre o teclado e a placa-mãe.
17:00	Consegui ler valores de correntes ao digitar cada tecla.
18:00	Término dos trabalhos do dia 26/11/2019.
09:20	Início dos trabalhos do dia 27/11/2019.
09:50	Colocando medidor de corrente no terminal que alimenta o terminal do mesário.
10:30	Identificou que durante uma votação ao retirar o teclado o sistema travou sem mensagem de erro.
12:15	Parada para almoço.
13:30	Reinício.
14:00	Identificou que a urna boota mesmo sem teclado conectado, dando o erro “Erro de Identificação de Hardware” no TM, sem especificar o problema.
15:00	Realizou o registro de 1 voto. Durante a votação do 2º eleitor foi desplugado o teclado. A urna travou. Religou a urna com o teclado. Votou pelo 2º eleitor. Iniciou a votação do 3º eleitor e retirou o cabo do display. Terminou o voto e encerrou a votação. A MR foi lida e não ha nos logs registros da retirada do teclado e vídeo.
17:50	Término dos trabalhos do dia 27/11/2019.

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador seguiu o plano proposto?
Sim
A infraestrutura solicitada/disponibilizada foi adequada?
Sim
As requisições foram atendidas adequadamente?
Sim

(Continuação)

CONCLUSÕES DO GRUPO DE ACOMPANHAMENTO
O grupo/investigador solicitou algo não contemplado no edital?
Não
Houve evolução diária no plano proposto?
Não. O investigador teve dificuldades de evoluir ao descobrir que o teclado da urna é blindado e cifrado. Ao plugar os sensores na urna, o investigador verificou que a sua ferramenta (sensor de arduino) não seria uma ferramenta adequada pra conseguir capturar o sinal USB (pouca precisão e baixa taxa de amostragem) e que haviam sinais capturados mesmo quando não se pressionava teclas.
Foram solicitadas alterações no plano proposto no decorrer de sua execução?
Não
Caso sim, estas alterações foram aprovadas e executadas?
Houve sucesso/achado na execução do plano proposto, considerando os objetivos estabelecidos no edital?
Não
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na segurança do processo eleitoral?
Não houve achado relativos à segurança. Porém durante a execução do teste, o investigador encontrou duas oportunidades de melhoria de usabilidade sendo uma relacionadas a uma mensagem de erro de falha do teclado e outra relacionada ao som emitido durante um reboot da urna.
Há algo a destacar nas atividades do grupo/investigador que possa agregar melhorias na execução de futuros Testes de Públicos de Segurança (TPS)?
Não

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES
Procedimento de votação e retirada do teclado.
Iniciamos o processo de digitalção do código do candidato e retiramos o teclado da máquina.
Não verificamos mensagem ou alteração no sistema relatando a retirada do hardware.
Encerramos a transmissão de energia através da chave Liga-Desliga e noamos a mensagem “Votação Suspensa” e o aúdio característico do término da votação.
Em outro procedimento, retiramos o teclado antes da votação e da mesma forma, não verificamos tratativa para a ocorrência.

(Continuação)

OBSERVAÇÕES DO GRUPO DE INVESTIGADORES
Com a retirada do flat de vídeo no memento da votação, com a tela desligada, conseguimos digitar o voto e ouvimos o sinal de áudio de confirmação.
Sobre o procedimento proposto, conseguimos gerar as leituras analógicas transmitidas pelo teclado mas não houve progresso na decodificação do sinal verificado.

_____

ASSINATURA DO COORDENADOR DO GRUPO DE INVESTIGADORES

_____

ASSINATURA DO RESPONSÁVEL PELO ACOMPANHAMENTO

Anexo G – Relatório final de acompanhamento das atividades

COMISSÃO REGULADORA

REPRESENTANTES DOS SECRETÁRIOS DE TI DOS TRIBUNAIS REGIONAIS ELEITORAIS

EQUIPE DE APOIO

RELATÓRIO FINAL DE ACOMPANHAMENTO DAS ATIVIDADES (relatório conjunto)

Considerações gerais sobre o TPS

- O TPS constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, apuração, transmissão e recebimento de arquivos;
- O TPS teve por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar aperfeiçoamento do processo eleitoral.
- Período do TPS: 25 a 29 de novembro de 2019
- Local: Sede do TSE – Brasília – DF
- Investigadores Participantes:
  - 5 (cinco) grupos de investigadores:
    - Grupo 1: especialistas não vinculados a nenhum órgão;
    - Grupo 2: especialistas do SENAC/Estácio;
    - Grupo 3: especialistas da Universidade Federal Fluminense – UFF;
    - Grupo 4: especialistas da Universidade de Taubaté – UNITAU;
    - Grupo 5: especialistas da Polícia Federal – DF.
  - 3 (três) investigadores individuais não vinculados a nenhum órgão.
  - A Tabela 1 anexa contém o detalhamento das equipes de investigação (grupos e individuais) com nome dos componentes e resumo do objetivo dos testes (plano de ataque).
- Equipe de apoio aos investigadores:
  - 13 (treze) integrantes dos seguintes órgãos:
    - INPE – Instituto Nacional Pesquisas Espaciais
    - CTI – Centro de Tecnologia da Informação Renato Archer
    - FACTI – Fundação de Apoio à Capacitação em Tecnologia da Informação (apoio ao MCTIC e CTI)
    - TRE-MG
    - TRE-PA
    - TRE-PB
    - TRE-SC

- A Tabela 2 anexa contém o nome dos componentes da equipe de apoio de cada órgão.

- Observadores representantes dos Tribunais Regionais Eleitorais:
  - 5 (cinco) Secretários de Tecnologia da Informação representando cada uma das regiões geográficas do Brasil:
    - Região Sul: TRE-PR
    - Região Sudeste: TRE-ES
    - Região Centro-Oeste: TRE-GO
    - Região Norte: TRE-RR
    - Região Nordeste: TRE-PB
  - A Tabela 3 anexa contém o nome dos Secretários de TI representantes de cada região.
- Equipes de apoio técnico no TSE e Regionais:
  - Técnicos do TSE e dos Tribunais Regionais envolvidos nos sistemas avaliados e na infraestrutura disponibilizada para o evento.

Considerações sobre os planos de ataque e evoluções alcançadas:

GRUPO 1:

- Plano de ataque: tentativa de manipulação do boletim de urna.
- Observações ao plano apresentado: o grupo executou suas atividades de acordo com o plano proposto, buscando a identificação de padrões dos registros dos votos no arquivo RDV, bem como falhas no processo envolvido, com objetivo de identificar o voto do eleitor.
- Principais achados:
  - não foram registrados achados durante os testes.
  - o registro completo das atividades do grupo está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

GRUPO 2:

- Plano de ataque: teste da urna eletrônica baseado em IA e processamento de sinais.
- Observação ao plano apresentado: o grupo executou suas atividades de acordo com o plano proposto.
- Principais achados:
  - não foram registrados achados durante os testes.
  - o registro completo das atividades do grupo está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

GRUPO 3:

- Planos de ataque:
  - Plano 1 - tentativa de obtenção de chaves criptográficas;
  - Plano 2 - verificar vulnerabilidades de bibliotecas do sistema.
- Observação aos planos apresentados:
  - Plano 1: o grupo executou suas atividades de acordo com o plano proposto.
  - Plano 2: o grupo executou suas atividades de acordo com o plano proposto.
  - Os pontos de ataque, aparentemente, foram baseados em achados dos TPS anteriores.
- Principais achados:
  - não foram registrados achados durante os testes.
  - o registro completo das atividades do grupo está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

GRUPO 4:

- Plano de ataque: Tentativa de mapeamento de rotina por meio de algoritmo de reconhecimento de padrão.
- Observações ao plano apresentado: o grupo executou suas atividades de acordo com o plano proposto.
- Principais achados:
  - não foram registrados achados durante os testes.
  - o registro completo das atividades do grupo está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

GRUPO 5:

- Planos de ataque:
  - Plano 1 - Extração do conteúdo do disco criptografado do SIS.
  - Plano 2 - Instalação e execução de código arbitrário em uma máquina do Gedai.
  - Plano 3 - Extração de dados e configurações do Kit JE Connect.
- Observações aos planos apresentados:
  - Plano 1: o grupo executou suas atividades de acordo com o plano proposto.
  - Plano 2: o grupo executou suas atividades de acordo com o plano proposto, e realizou atividades adicionais para ampliar o escopo do ataque, com objetivo de subverter o funcionamento do Gedai.

- Plano 3: o grupo executou algumas atividades de acordo com o plano, restringindo-se a estudos do ambiente.

- Principais achados:
  - Plano 1: os investigadores alcançaram êxito na extração do conteúdo do disco cifrado pelo SIS, inclusive removendo o SIS do ambiente.
  - Plano 2: os investigadores alcançaram êxito na instalação e execução de programas em uma máquina do Gedai. A partir do código fonte do sistema disponibilizado foi identificado o conjunto de caracteres (string) que criptografa a "chave privada" do Gedai. A partir dos arquivos existentes foram gerados arquivos adulterando nome de município. Estes arquivos adulterados foram transferidos para Urna Eletrônica. A Urna Eletrônica inicializou, e os arquivos adulterados foram aceitos.
  - Plano 3: não houve êxito.
  - o registro completo das atividades do grupo está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

INVESTIGADOR INDIVIDUAL 1:

- Plano de ataque: Exploração de vulnerabilidades na infraestrutura de redes, sistemas e ativos.
- Observação ao plano apresentado: o investigador executou suas atividades de acordo com o plano proposto.
- Principais achados:
  - não houve êxito nas questões de segurança;
  - o investigador identificou duas possíveis melhorias de usabilidade na urna, durante o processo de votação.
  - o registro completo das atividades do investigador está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

INVESTIGADOR INDIVIDUAL 2:

- Plano de ataque: Teste de invasão utilizando análise de pulso elétrico.
- Observação ao plano apresentado: o investigador executou suas atividades de acordo com o plano proposto, buscando a quebra de sigilo do voto, utilizando análise de sinais elétricos dentro da urna.
- Principais achados:
  - não houve êxito nas questões de segurança;
  - o registro completo das atividades do investigador está contido no respectivo relatório elaborado pelo grupo de apoio, em anexo.

INVESTIGADOR INDIVIDUAL 3:

- Plano de ataque:
  - 1 - Teste de Integridade da coleta de votos
  - 2 - Teste de integridade do arquivo de votos
  - 3 - Integridade do arquivo executável da urna
- Observação ao plano apresentado:
  - Plano 1: investigador não compareceu.
  - Plano 2: investigador não compareceu.
  - Plano 3: investigador não compareceu.
- Principais achados:
  - investigador não compareceu.

Considerações finais:

A Comissão Reguladora, o Grupo de Apoio e os Secretários de TI representantes do Tribunais Regionais Eleitorais presentes ao TPS consideram que o objetivo “de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição e apresentar as respectivas sugestões de melhoria” foi plenamente atingido.

Os relatórios detalhados anexos a este documento serão encaminhados para a Comissão Avaliadora, a qual cabe emitir parecer sobre os resultados alcançados por cada grupo/investigador.

O ambiente disponibilizado pelo TSE para a execução dos testes foi considerado adequado por todos os grupos/investigadores.

As equipes técnicas do TSE e Regionais deram suporte adequado ao serem demandadas, atendendo a contento as requisições dos grupos/investigadores.

Anexo H – Relatório da Comissão Avaliadora

Relatório Final da Comissão Avaliadora

1. Introdução

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

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

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

O propósito deste relatório 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 2017, 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

Foram recebidos 14 planos de teste e aprovados 13. Compareceram 5 grupos de investigadores e 2 investigadores individuais, sendo executados efetivamente 10 planos de teste. Os objetos das propostas foram os seguintes:

3.1) Grupo de Investigadores: ***Fellipe Ribeiro Silva Abib (Coordenador)***

- Componentes do Grupo: Alan Papafanurakis Heleno, Caio Henrique de Aquino, Vicente Charles Willian Biesseki.
- Plano de Teste: identificação do eleitor e de seu voto a partir das informações gravadas no Registro Digital do Voto (RDV) e tentativa de manipulação do Boletim de Urna (BU).

3.2) Grupo de Investigadores: ***Jairo Simão Santana Melo (Coordenador)***

- Componentes do Grupo: Felipe Pradera Resende, Luiz Fernando Sirotheau Serique Junior, Leonardo de Almeida Ramos.
- Plano de Teste: identificação da operação eletrônica da urna, analisando os sinais elétricos nos circuitos entre o teclado e a placa mãe, empregando técnicas de inteligência artificial para identificação de cada tecla pressionada.

3.3) Grupo de Investigadores: ***Luis Antonio Brasil Kowada (Coordenador)***

- Componentes do Grupo: Gabriel Cardoso de Carvalho, Victor Faria de Souza, Igor Palmieri Antunes (ausente), Ramon Rocha Rezende.
- Plano de Teste 1: obtenção de chaves criptográficas e verificação do correto uso da criptografia para a garantia da integridade, confidencialidade e autenticidade.
- Plano de Teste 2: verificar a proteção de programas pré-construídos (denominados de bibliotecas), necessários ao sistema da urna.

3.4) Grupo de Investigadores: ***Luís Fernando de Almeida (Coordenador)***

- Componentes do Grupo: Fábio Rosindo Daher de Barros, Gabriel Ferrari Carvalho, Josinei Rodrigues Lopes Silva, Fernando Nogueira da Silva.
- Plano de Teste: tentativa de uso de Machine Learning para reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

3.5) Grupo de Investigadores: *Paulo César Herrmann Wanner (Coordenador)*

- Componentes do Grupo: Ivo de Carvalho Peixinho, Galileu Batista de Souza.
- Plano de Teste 1: recuperação de senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos.
- Plano de Teste 2: quebra da criptografia da proteção (SIS) do sistema gerador de mídia das urnas eletrônicas (GEDAI).
- Plano de Teste 3: domínio do sistema de geração de mídia a fim de adulterar dados de preparação da urna da seção eleitoral.

3.6) Investigador Individual: *José Fellipe de Moraes Albano*

- Plano de Teste: identificação de componentes da rede computacional do TSE de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede.

3.7) Investigador Individual: *Leonardo Cunha dos Santos*

- Plano de Teste: quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas.

4. 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:

4.1) Planos de teste não realizados

Grupo Paulo César Herrmann Wanner: o Plano de Teste 3, descrito como "recuperar senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos", não foi executado por não ter obtido sucesso na tentativa de execução do programa de transmissão em um ambiente virtual para a sua manipulação. Os esforços técnicos foram dedicados aos seus planos de teste 1 e 2.

4.2) Planos de teste realizados sem contribuições

a. Grupo Fellipe Ribeiro Silva Abib: identificação do eleitor e seu voto a partir do posicionamento dos votos gravados no RDV.

   Justificativa: Os investigadores verificaram os código-fontes dos programas de votação e geração de Boletim de Urna, realizaram algumas votações na urna para verificação da lógica implementada, mas não conseguiram passar pelos mecanismos de segurança para identificar o voto e efetuarem as alterações desejadas.

b. Grupo Jairo Simão Santana Neto: levantar a influência da operação eletrônica da urna, em decorrência de se pressionar suas teclas.

   Justificativa: Os investigadores tiveram acesso aos circuitos elétricos da urna para conectar um osciloscópio para leitura dos sinais elétricos gerados pelo teclado, mas não conseguiram identificar padrões, nesses sinais observados, no intuito de obter as informações necessárias com objetivo de identificar as teclas pressionadas e, consequentemente, o voto.

c. Grupo Luis Antonio Brasil Kowada (Plano de Teste 1): obtenção de chaves criptográficas e avaliar o uso da criptografia para a garantia da integridade, confidencialidade e autenticidade.

   Justificativa: Os investigadores tentaram obter as chaves criptográficas empregando as técnicas utilizadas no TPS anterior e atestaram que os ajustes de segurança implementados não possibilitaram concluir os objetivos propostos.

d. Grupo Luis Antonio Brasil Kowada (Plano de Teste 2): verificar a proteção de programas pré-construídos, necessários ao sistema da urna.

   Justificativa: Foram observados que todos os programas e dados carregados na urna estavam protegidos, não permitindo realizar ou introduzir qualquer alteração.

e. Grupo Luis Fernando de Almeida: analisar a possibilidade de criar rotinas inteligentes, utilizando as técnicas de Machine Learning, capazes de reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

   Justificativa: Os investigadores realizaram uma sequência de votação conhecida para identificar alguma correlação com o registro dos votos na urna. No entanto, não lograram sucesso.

f. Investigador José Fellipe de Moraes Albano: identificação de componentes da rede computacional do TSE de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede.

Justificativa: Os testes ficaram limitados aos enlaces de comunicação para a transmissão do Boletim de Urna. Todas as tentativas de intervenção nos sistemas de conectividade à rede não foram concluídas.

g. Investigador Leonardo Cunha dos Santos: quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas.

Justificativa: O investigador realizou algumas intervenções na urna para realizar uma leitura dos sinais elétricos do teclado e, apesar de não ter obtido sucesso no processo de identificação da tecla digitada pelo eleitor, identificou que a urna fica inoperante quando o teclado é desconectado. No entanto, a urna não reporta explicitamente o motivo da falha, muito embora seu sistema operacional continue atuante e registrando eventos.

4.3) Planos de teste realizados com contribuição

a. Grupo Paulo César Herrmann Wanner (Plano de Teste 1): quebrar a criptografia da proteção do sistema gerador de mídia das urnas eletrônicas.

i. Contribuição:
O GEDAI (Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica) é responsável por gerar os cartões de instalação das urnas eletrônicas. Quando o GEDAI é executado no ambiente do sistema operacional Windows ele fica sob um programa chamado SIS (Subsistema de Instalação e Segurança) que tem o objetivo de proteger o computador utilizado pela Justiça Eleitoral. O SIS cifra a unidade de armazenamento onde o GEDAI está instalado, utilizando o programa TrueCrypt, constituindo um primeiro nível de barreira de segurança. Neste volume cifrado estão contidos todos os programas, arquivos de configuração e algumas chaves criptográficas utilizadas pelo GEDAI. A chave utilizada para abrir a unidade de armazenamento cifrado é gerada no momento da instalação, por meio de um algoritmo proprietário do TSE.
Como o equipamento é preparado de forma a ser replicado e instalado em todos os ambientes da Justiça Eleitoral para preparação da urna eletrônica, a cifra não pode ser atrelada ao usuário do sistema em cada

instância da máquina, já que os usuários são da ordem de centenas a milhares, com inevitável rotatividade, tornando inviável a administração de senhas individuais neste cenário. Sendo assim, a senha é gerada durante a instalação e configuração do equipamento, e por princípio fica armazenada no próprio dispositivo de armazenamento da máquina. É fato, portanto, que um invasor, dispondo dos conhecimentos e das técnicas necessárias, poderá obter a chave de cifragem. A eficácia desta proteção é limitada, mas exerce seu papel de barreira suplementar inicial, exigindo tempo e trabalho técnico em uma eventual tentativa de ataque.

Tendo eliminado a barreira da cifragem, a equipe abriu um caminho para tentar ataques contra o próprio SIS para ter o acesso ao GEDAI e as informações associadas.

A equipe demonstrou a esperada viabilidade de se recuperar a senha, gastando pouco mais de um dia de trabalho para seu êxito. Há de se ressaltar que a equipe já atuou nos eventos anteriores do TPS e conhecia com profundidade o sistema a ser atacado, o que contribuiu de sobremaneira o processo.

ii. Impactos:

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

iii. Extensão:

O ataque expõe o sistema gerador de mídia, sem a proteção do sistema hospedeiro, ou, em outras palavras, expõe o sistema que grava o software da urna na mídia utilizada para instalação, normalmente pertencentes a uma zona eleitoral, que pode abranger um município de pequeno porte ou parte de um município de grande porte.

iv. Contexto:

A inseminação do software das urnas ocorre nas dependências da Justiça Eleitoral (TRE e Cartórios Eleitorais) por pessoal qualificado e autorizado pelo TRE. O evento é previsto no calendário eleitoral, em um ritual público e com a presença de testemunhas de partidos políticos e da sociedade, além de gerar uma ata e relatório eletrônico das urnas inseminadas durante o processo.

b. Grupo Paulo César Herrmann Wanner (Plano de Teste 2): recuperar senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos.

i. Contribuição:

Após o sucesso na execução do plano de teste precedente, a equipe passa à tentativa de ataque ao sistema SIS propriamente dito, de forma a tentar neutralizá-lo e assim o acesso total à aplicação GEDAI, que seria o alvo principal para conseguir alterar o software e os dados que serão instalados no conjunto de urnas de uma zona eleitoral.

Desprovido da cifragem, o conteúdo da mídia de armazenamento do equipamento que roda SIS/GEDAI foi executado como máquina virtual e a equipe concentrou-se em manipular o Registro do sistema operacional Windows, local onde se armazena diversas configurações deste sistema operacional e de suas aplicações, para conseguir neutralizar o SIS. Após conveniente manipulação do registro, a equipe teve sucesso em iniciar a máquina virtual com o sistema SIS neutralizado e assim o acesso direto à aplicação GEDAI.

O SIS faz uma validação de assinatura digital de todos os programas que são executados, mas como ele foi neutralizado, esta validação não foi mais realizada, de modo que foi possível realizar alterações no executável do GEDAI.

A equipe conseguiu executar a aplicação GEDAI sob seu controle, porém as tentativas de gerar alterações no conteúdo a ser inserido na mídia de inseminação das urnas, a própria aplicação GEDAI rejeitou os código/dados alterados, gerando uma condição na urna de não inicialização ou execução correta do seu sistema.

Restringindo severamente as modificações nos arquivos a equipe finalmente conseguiu gerar uma versão de dados que a urna conseguiu executar. A urna, assim configurada, gerou uma zerézima e após a execução dos procedimentos de votação e da finalização gerou um Boletim de Urna (BU) aparentemente válido, sob o aspecto visual do mesário.

As alterações realizadas se limitaram ao nome do município e à Unidade da Federação (UF). No entanto, tais informações são impressas na zerézima e no BU apenas para o controle humano, sendo que os dados efetivamente utilizados na totalização são os códigos numéricos que identificam estes atributos, os quais não puderam ser alterados em função dos mesmos fazerem parte do conjunto de dados

assinados digitalmente pelo TSE e TRE. A Alteração desses códigos gera uma rejeição dos mesmos pelo software da urna em sua verificação inicial, uma vez que a urna realiza a verificação de assinatura dos mesmos.

ii. Impactos:

Os dados de nome do município e da UF que são impressos na zerézima e no BU foram alterados, mas não impactaram no sigilo e contabilização do voto. Esta pequena alteração descritiva dos dados não reflete em uma alteração real do município e UF, onde o voto é registrado, já que a integridade do código se manteve. O sistema de verificação prévia da assinatura de dados da urna não permitiu alteração que pudesse ser prejudicial à contabilização e ao sigilo do voto. O comportamento observado da urna nesta situação é a sua completa inatividade, sem nenhuma condição de operação visível, do ponto de vista do observador externo.

iii. Extensão:

O escopo do ataque é limitado às urnas da zona eleitoral pertinente, contudo há diversos pontos de verificação no processo eleitoral em que a verificação visual ocorre, a começar pelo próprio dia da inseminação. Eventualmente, falhas humanas em tais processos poderiam permitir a preparação de uma urna adulterada chegar à seção eleitoral no dia da eleição, o que certamente atrairia a atenção dos mesários, gerando substituição imediata da urna. Em última análise, caso nem mesmo os mesários notem a adulteração no nome do município e na UF, a votação será realizada sem problemas, com a contabilização correta dos votos e posterior "upload" ao sistema de totalização, sem gerar pendências. Apenas a versão da zerézima e do BU impressas pela urna trarão os nomes do município e UF adulterados.

iv. Contexto:

Há diversos procedimentos públicos, com testemunhas, desde a preparação da urna até o próprio dia da eleição. Diversos agentes dos procedimentos devem contribuir na verificação de conformidade comportamental e visual da urna, mas mesmo que todos falhem sequencialmente na detecção da anomalia, a votação em si não será afetada e tecnicamente a fraude não será consumada.

4.4) Contribuição extra-plano registrada pelos investigadores

a. Alteração do som emitido pela urna eletrônica para os eventos não relacionados à conclusão do voto.

Contribuição:

O investigador reporta que, durante seus testes, notou que a urna, durante sua preparação do início da votação, emite muitas vezes aquele já tradicional som, que aqui chamaremos “som padrão de término de votação”. Tal som é aquele emitido também quando um eleitor conclui o seu voto, que pode ser ouvido pelos mesários e pelos eleitores que estejam relativamente próximos ao local da votação.

O investigador sugere que a emissão desse “som padrão” durante os estágios de preparação, ou manuseio das urnas, no dia da votação pode sugerir aos eleitores eventualmente aguardando na fila o início da votação, de que algum tipo de manipulação de voto na urna possa estar ocorrendo, até mesmo que um conluio de mesários esteja proporcionando uma inserção de votos ilegalmente.

A Comissão Avaliadora concorda com a observação e recomenda que o som emitido durante a inicialização no dia da votação, término da votação, e mesmo nos procedimentos que precedem o dia da votação, seja alterado por um outro absolutamente diferenciado do “som padrão de término de votação”.

b. Remoção do cabo do teclado.

Contribuição

O investigador, durante testes internos da urna, observou que a remoção do cabo do teclado causa o "travamento" da urna. Muito embora a urna continue operando internamente, como pode ser comprovado pelo registro de eventos do sistema, o software atualmente falha em não reportar externamente, no display, a falha específica de mau contato do cabo do teclado. Dentre as falhas observadas em campo, possivelmente alguns casos são devidos ao eventual mau contato deste cabo, especialmente no caso das urnas que têm que ser transportadas a locais remotos para votação.

A sugestão é de que a urna registre no display este caso específico de problema, o que poderá auxiliar as equipes de manutenção no futuro. A urna deverá continuar inoperante, apesar do aviso, mas sem mostrar apenas uma tela branca, o que é bastante desconcertante quando acontece no dia da votação.

5. Recomendações dos Testes Anteriores

As recomendações contidas no Relatório Final da Comissão Avaliadora do TPS/2017 foram objeto de análise dessa comissão, inclusive com realização de reunião com representantes da Secretaria de Tecnologia da Informação/DG/TSE. Após a apresentação da secretaria mencionada, foi fornecida informação atualizada com as providências tomadas, conforme segue abaixo.

5.1) Alterar o nome do Termo de Confidencialidade para Termo de Responsabilidade

O TSE atendeu esta recomendação.
O documento agora é chamado "Termo de Responsabilidade", conforme expresso em edital. Resta pendente ajuste na Resolução, cujo processo (2019.00.000004566-6) está em tramitação.

5.2) Alterar a frase do item 3 do termo de confidencialidade de “bem como obter acesso aos sistemas com o objetivo de copiá-los” para “bem como obter acesso aos sistemas sob análise com o objetivo de copiá-los e/ou transportá-los”

O TSE atendeu esta recomendação.

O Termo de Responsabilidade do TPS/2019 apresenta a redação proposta.

5.3) Alterar a frase do item 7 do termo de confidencialidade de “ou qualquer outro dispositivo de computação móvel” para “ou qualquer outro dispositivo computacional”

O TSE atendeu esta recomendação.

O Termo de Responsabilidade do TPS/2019 apresenta a redação proposta.

5.4) Instituição de um Comitê de Assessoria Perene

O TSE não atendeu esta recomendação.

O tema foi submetido à Comissão Reguladora e esta entendeu que a decisão pela criação da Comissão de Assessoria Perene é de competência da alta administração do TSE. O tema foi submetido. No processo SEI 2019.00.000004566-6, foi incluído o Relatório da Comissão Avaliadora do Teste Público de Segurança 2017 (SEI 1030110) e nele consta, como recomendação, a "Instituição de um Comitê de Assessoria Perene".

5.5) Tornar o exame do software da urna perene e constante, mas mantendo o TPS no formato em que está

O TSE não atendeu esta recomendação.

Existe um projeto novo para abertura do código-fonte, o software da urna, que está em avaliação quanto à viabilidade jurídica. A Portaria TSE nº 444, de 10 de junho de 2019, institui comissão para realizar estudos relativos à viabilidade da publicação do código-fonte do conjunto de software do ecossistema da urna eletrônica na Internet. Para esta eleição, os investigadores poderão acompanhar as alterações dos códigos-fonte após o reteste.

5.6) Estender o TPS para cobrir não apenas ataques computacionais, mas também ataques de engenharia social

O TSE não atendeu esta recomendação.

A Comissão Reguladora entende que o TPS se presta ao exercício dos sistemas eleitorais.

5.7) Estender o TPS para testar elementos em maior profundidade, removendo barreiras existentes de forma a tornar mais eficientes os testes, dado o curto período de tempo disponível

O TSE não atendeu esta recomendação.

A Comissão Reguladora poderá estudar meios de facilitar a realização dos testes pelos investigadores. Não haverá alterações quanto às barreiras de segurança, a flexibilização dessas é desnecessárias para a realização dos ataques.

5.8) Realização de auditorias cientificamente embasadas

O TSE atendeu esta recomendação.

Existe um grupo do TSE (GT – Auditoria, instituído pela Portaria TSE nº 1056, de 05 de dezembro de 2018) realizando estudos para a melhoria das fiscalizações e auditorias do processo eleitoral para o pleito de 2020. As propostas, uma vez concluídas, serão

submetidas ao Ministro relator das resoluções e também submetidas à audiência pública.

5.9) Garantia do acompanhamento das correções do software

O TSE atendeu esta recomendação.

Além da realização do reteste, caso a proposta seja acatada pelo Ministro relator, os investigadores poderão acompanhar a evolução do código-fonte. O reteste está previsto na Resolução TSE nº 23.444, de 30 de abril de 2015, e a minuta de Resolução de Fiscalização e Auditoria, processo SEI 2019.00.000011039-5, prescreve o acesso aos códigos-fonte, nos 6 meses que antecedem o pleito.

5.10) Estudo de ataques via artefatos no processo de compilação

O TSE atendeu esta recomendação.

Foi incluída, na minuta de Resolução de Fiscalização e Auditoria (processo SEI 2019.00.000011039-5), previsão para procedimento de análise dos binários produzidos durante a compilação, com vistas a verificar a sua correspondência ao código-fonte analisado. Além disso, os compiladores utilizados na lacração são de código aberto e amplamente utilizados pela comunidade. Os compiladores são lacrados com o software produzido pelo TSE.

5.11) A lacração dos sistemas deve ocorrer antes do TPS

O TSE atendeu esta recomendação.

Os sistemas submetidos ao TPS são lacrados um mês antes da realização dos testes.

5.12) O TPS deve abranger os sistemas de totalização e biometria

O TSE não atendeu esta recomendação.

As sugestões, no momento, não poderão ser acatadas, haja vista que o sistema RecBU está sendo reescrito para as eleições de 2020 e deverá estar disponível para o TPS 2021. Quanto ao sistema de biometria, da mesma forma, ainda há uma indefinição quanto ao software a ser utilizado nas próximas eleições: Bozorth ou Griaule.

5.13) Eliminar a restrição etária para participação no TPS

O TSE não atendeu esta recomendação.
A responsabilidade penal do participante impossibilita esta opção. Esta questão foi apresentada à Administração (processo SEI 2019.00.000004566-6 – Informação ASSEC nº 23/2019, SEI 1135984).

6. Recomendações

6.1) Atender as recomendações apresentadas por esta Comissão Avaliadora em seus Relatórios de Avaliação elaborados ao final dos Testes Públicos de Segurança anteriores.

6.2) 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.

6.3) 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.

6.4) Quanto ao processo de desenvolvimento:

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 a 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.

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.

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 tais princípios.

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.

6.5) Quanto ao código fonte:

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.

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.

6.6) Quanto ao processo de inscrição e de seleção:

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).

6.7) Quanto à ampliação do objeto do TPS:

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.

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/TREs e estabelecendo uma "cabeça de ponte" para o atacante elaborar ataques precisos e sofisticados contra alvos internos geralmente desprotegidos das ferramentas usuais de defesa.

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.

6.8) Quanto ao ambiente de realização do TPS:

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.
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 vídeo-chamadas, 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.

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.

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.

6.9) Quanto às modificações nos sistemas objeto do TPS

a. O ataque à cifragem da mídia de armazenamento do sistema GEDAI revelou que a barreira implementada pelo sistema 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).

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 conclui 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.

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.

6.10) 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.

Brasília/DF, 10 de dezembro de 2019.

COMISSÃO AVALIADORA DO TESTE PÚBLICO DE SEGURANÇA 2019

Anexo I – Certificado de participação

TPS 2019
TESTE PÚBLICO DE SEGURANÇA

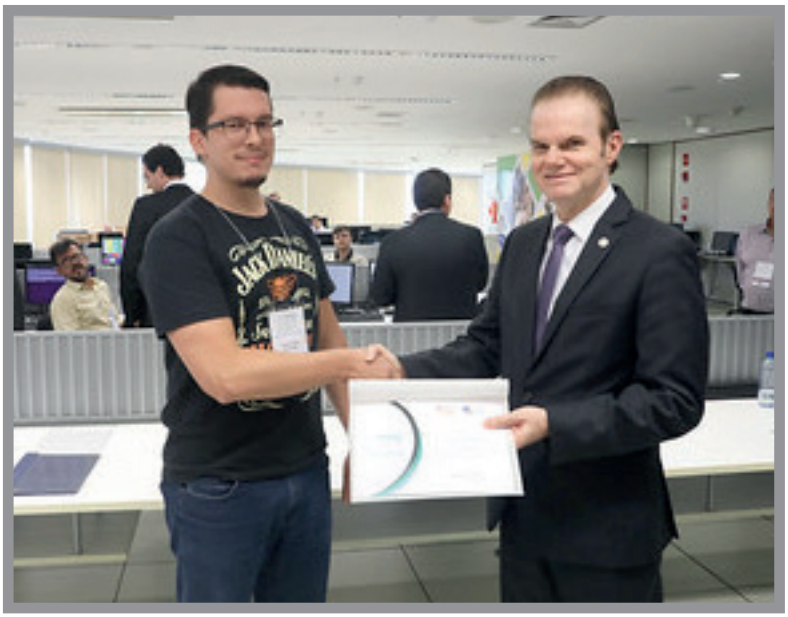
#SEUVOTOTEMPODER ELEIÇÕES 2020

Tribunal Superior Eleitoral

Certifico que

participou, como investigador, do Teste Público de Segurança do Sistema Eletrônico de Votação, realizado no período de 25 a 29 de novembro de 2019, na sede do Tribunal Superior Eleitoral.

MINISTRA ROSA WEBER
Presidente
Tribunal Superior Eleitoral



Esta obra foi composta na fonte Helvetica, corpo 11 e
entrelinhas de 14 pontos.