



Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

Relatório dos resultados da realização dos Testes Públicos

Grupo 02

Representando a UnB – Universidade de Brasília

Lauro Cesar Araújo – Mestre em Arquitetura da Informação – UnB

Sérgio Freitas da Silva – Pós-graduado em Ciência da Computação - ESAB

Plano de Teste G2PT2

Fraude no Sistema de Apuração utilizado no exterior

Conteúdo deste relatório

1. Plano de Testes original, submetido pelos Investigadores
2. Acompanhamento dos fatos pela Equipe de Apoio
3. Resultados do Teste
4. Conclusões
5. Futuras Possibilidades

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título do Plano de Teste	Fraude no Sistema de Apuração utilizado no exterior
Instituição Proponente	Universidade de Brasília
Responsável (nome, e-mail e telefone do autor ou responsável)	Lauro César Araújo (laurocesar@gmail.com) Sérgio Freitas da Silva (sergio.freitas.silva@gmail.com)
Sistemas Afetados	Software: <input checked="" type="checkbox"/> Software de votação usado nas seções eleitorais Hardware: <input type="checkbox"/> Microterminal <input type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input type="checkbox"/> Mídias Procedimentos: <input type="checkbox"/> Geração de mídias <input type="checkbox"/> Etapas de preparação da urna <input checked="" type="checkbox"/> Votação
Duração Estimada do Teste (em minutos)	30 minutos
Extensão do ataque	<input type="checkbox"/> Urna ou seção eleitoral <input type="checkbox"/> Local de votação <input type="checkbox"/> Zona eleitoral <input type="checkbox"/> Município <input type="checkbox"/> Unidade da Federação <input checked="" type="checkbox"/> País
Conhecimentos necessários	Operação do Sistema de Apuração

Observações:

- O teste a ser realizado deve ser, obrigatoriamente, reproduzível.
- Este plano deverá ter no máximo 10 páginas em formato A4 ou Carta.

2 Reservado ao Tribunal Superior Eleitoral (TSE)

Protocolo	Data
	Resultado <input type="checkbox"/> Aprovado <input type="checkbox"/> Aprovado com ressalvas <input type="checkbox"/> Reprovado



3 Detalhamento do teste

3.1 Resumo do teste

Conforme esquematizado abaixo, o teste consiste na fraude do Sistema de Votação Eletrônica utilizado no exterior. O Sistema de Apuração pode ser utilizado como contingência no caso de falha do sistema de votação principal. No Sistema de Apuração utilizado no exterior (Figura 1), as informações do Boletim de Urna (1) podem ser adulteradas durante o processo de digitação do Boletim da Urna (2) utilizando-se um código verificador genérico (3).



Figura 1 – Sistema de Apuração no exterior

O objetivo do teste é demonstrar a vulnerabilidade do Sistema de Apuração executado no exterior ao utilizar um código verificador genérico para validar os dados do Boletim de Urna digitados durante o processo de apuração.

3.2 Fundamentação

O Sistema de Apuração está previsto na legislação eleitoral vigente (Resolução 23.372, de 14/12/2011) e consiste basicamente num mecanismo de contingência para recuperação dos dados da urna em casos de falhas do sistema.

O procedimento previsto nesse plano de teste aplica-se ao processo de votação no exterior e, portanto, não há previsão oficial de utilização nesse ano de 2012. Todavia, recomenda-se expressamente a realização do teste considerando que a vulnerabilidade encontra-se implementada na versão atual e, caso não seja prontamente corrigida, pode ser explorada inclusive nas próximas eleições.

Durante a fase de preparação, ao analisar o código-fonte disponibilizado, analisar os Boletins de Urna e entrevistar a equipe de desenvolvimento, os investigadores obtiveram as seguintes informações:

- O Boletim de Urna possui um Código Verificador (de cinco dígitos) utilizado para verificar a integridade dos dados impressos no Boletim (Zona, Seção, Candidato, Votos, etc.);
- O Sistema de Apuração utiliza esse Código Verificador para verificar a integridade dos dados digitados durante o processo de apuração;
- O Sistema de Apuração também pode ser utilizado no exterior, nesse caso, a Unidade Federativa (UF) da urna é equivalente ao texto "ZZ";
- Existe um Código Verificar genérico é utilizado para verificar a integridade dos dados digitados durante a apuração da Unidade Federativa "ZZ" (internacional);

Destarte, diante das informações obtidas, é possível inferir que a utilização do Sistema de Apuração no exterior (UF ⇔ ZZ) admite a adulteração dos dados durante a digitação do Boletim de Urna por meio da utilização de um Código Verificador genérico.

3.3 Precondições para o teste

Para realização dos testes será necessária a utilização dos seguintes recursos materiais:

- Uma eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF = "ZZ");
- Boletim de Urna válido impresso e disponível para digitação no Sistema de Apuração;

3.4 Escopo – Superfície de Ataque

O ataque consiste na utilização de um código verificador genérico para validar os dados do Boletim de Urna digitados incorretamente durante o processo de apuração (no exterior, ou seja, UF ⇔ "ZZ")

Os seguintes componentes do sistema de votação eletrônica sofrerão atuação durante o teste:

- Material: Uma eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF = "ZZ");
- Procedural: simulação do processo de apuração no exterior com digitação do Boletim de Urna;



3.5 Janela de atuação simulada do atacante

A atuação do atacante deve ocorrer nos seguintes instantes:

- Acesso à urna eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF = "ZZ");
- Digitação do Boletim de Urna no Sistema de Apuração;
- Utilização de um Código Verificador genérico para validar dados inconsistentes digitados propositalmente durante o processo de apuração;

3.6 Pontos de intervenção

O único ponto de intervenção é a digitação do Boletim de Urna no Sistema de Apuração configurado para votação no exterior.

3.7 Passos a serem realizados e Material Necessário

O processo é detalhado abaixo:

- Início do teste;
- O atacante recebe o Boletim de Urna válido impresso e disponível para digitação no Sistema de Apuração;
- O atacante recebe a Urna eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF = "ZZ");
- O atacante simula um processo de apuração digitando incorretamente alguns dados do Boletim de Urna, conforme solicitado pela interface do Sistema de Apuração;
 - Duração estimada: 5 minutos
- O atacante digita um Código Verificador genérico para validar a entrada de dados;
 - Duração estimada: 5 minutos
- O atacante verifica que o Sistema de Apuração validou os dados inconsistentes com a utilização do Código Verificador genérico;
 - Duração estimada: 5 minutos
- Fim;

Critério de parada:

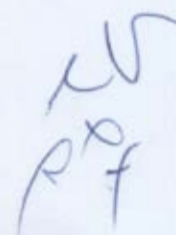
- Verificação de que o Sistema de Apuração validou os dados inconsistentes com a utilização de um Código Verificador genérico;

Tempo total estimado:

- 15 minutos;

Materiais necessários:

- Boletim de Urna válido impresso e disponível para digitação no Sistema de Apuração;
- Urna eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF = "ZZ");



3.8 Possíveis resultados e impacto

Os resultados esperados são os seguintes:

- Tipo do resultado esperado:
 - Validação de dados inconsistentes com a utilização de um Código Verificador genérico no Sistema de Apuração;
- Impacto:
 - Fraude eleitoral com adulteração dos votos;
- Extensão do ataque:
 - Exterior

Nas condições do teste, mantida a mesma versão do código-fonte visualizada durante a fase de preparação, estimamos a probabilidade de sucesso do ataque em 100%.

3.9 Rastreabilidade

A princípio, o ataque pode ser rastreado a partir da verificação do processo de digitação do Código Verificador e, posteriormente, pela simples conferência dos dados digitados.

Todavia, Se o processo descrito no teste puder ser utilizado fora do ambiente controlado pela Justiça Eleitoral, Então, em tese, seria possível gerar Boletins de Uma legítimos a partir de dados falsos.

3.10 Solução proposta

Para solucionar o problema identificado no plano de teste sugerem-se as seguintes alternativas:

Solução 1) Eliminação de um Código Verificador genérico implementado no código;

Solução 2) Utilização de uma chave específica para o exterior (UF↔ZZ), semelhante ao processo utilizado na geração do Código Verificador para as demais Unidades da Federação;

Nota final:

Este plano de testes contém informações sensíveis de segurança da informação. Recomendamos a gestão adequada destas informações para evitar prejuízos materiais e institucionais relacionados à sua má utilização.





Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
G2PT2	Coordenador:	Lauro Cesar Araujo	
	Investigador 1:	Sergio Freitas da Silva	

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	11:48	Hora de Término:	12:10
Resp. Acomp.:	Pedro Henrique Matheus da Costa Ferreira			Rubrica:	

Dados do Teste		
Titulo do teste:	Fraude no sistema de apuração utilizado no exterior	
Início do teste (Data/Hora):	22/03/2012	11:48
Termino do teste (Data/Hora):	22/03/2012	12:10
Critério de Parada:	Verificado que o sistema de apuração valida os dados inconsistentes com o boletim de urna dada a utilização do código verificador genérico.	

Relaxamento nos mecanismos e procedimentos de segurança
Falta de idoneidade do digitador, e a falta de atenção das pessoas responsáveis pela conferência dos dados digitados na urna eletrônica.

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	O Atacante recebe o Boletim de Urna válido impresso e disponível para digitação no sistema de apuração	
2	O Atacante recebe a Urna Eletrônica com programas carregados, configurada e disponível para execução do sistema de apuração (configurada para Exterior, ou seja, UF = "ZZ");	
3	O Atacante simula um processo de apuração digitando incorretamente alguns dados do Boletim de Urna, conforme solicitado pela interface do sistema de apuração	
4	O Atacante digita um Código Verificador genérico para validar a entrada de dados	
5	O Atacante verifica que o sistema de apuração validou os dados inconsistentes com	

	a utilização do Código Verificador genérico.	
6	Fim	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
11:48	Não foi possível disponibilizar uma Urna Eletrônica com programas carregados, configurada e disponível para execução do Sistema de Apuração (configurada para o Exterior, ou seja, UF="ZZ"); nenhum BU válido impresso e disponível para digitação no sistema de apuração. Isso é justificado pelo fato de as próximas eleições não contemplarem votação no exterior, ou seja, não contempla o cargo de Presidente da República.
11:50	O investigador solicitou acesso à documentação técnica de requisitos de software do Sistema de Apuração. A solicitação não pode ser atendida no prazo restante para a conclusão do teste.
11:55	Como forma alternativa de execução dos testes, o investigador teve acesso ao código-fonte do sistema como meio de averiguar a hipótese levantada no Plano de Teste. Pela análise lógica das instruções dos programas, evidenciou-se que é possível substituir o Código Verificador do BU impresso por uma sequência específica padrão de dígitos numéricos que possibilita que um BU adulterado seja considerado válido pelo sistema.
12:10	Essa demonstração tornou desnecessária a disponibilização da Urna Eletrônica e do BU impresso nos moldes solicitados no plano de teste.

Conclusões sobre o teste
A hipótese levantada no Plano de Teste se mostrou verdadeira com base na análise do código-fonte. O teste demonstra que existe um ponto de melhoria possível no processo de apuração de contingência de urnas utilizadas no exterior.

Considerações do grupo investigador
O grupo investigador sugere que alterações sejam realizadas nos processos, procedimentos e requisitos do software para que a fragilidade identificada seja eliminada. Sugere-se também que uma revisão completa do código-fonte seja realizada e que processos de desenvolvimento de software sejam auditados.

Considerações do grupo de apoio
O teste transcorreu sem problemas ou ocorrências.



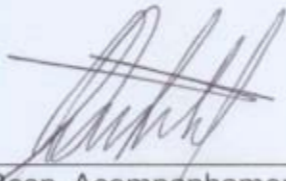

Futuras Possibilidades
Como possibilidade futura, sugere-se providenciar auditoria dos códigos-fontes e a revisão dos requisitos funcionais do sistema.

Alinhamento do PT
Não foi possível executar os testes diretamente no software de Apuração conforme descrito na seção "Acompanhamento dos Procedimentos".

Informações Adicionais
Não Há



Lauro Cesar Araujo

Sergio Freitas da Silva

Resp. Acompanhamento
Pedro H. Matheus

P/ Luiz Otavio Duarte