



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 01

Diego de Freitas Aranha – Doutor em Ciência da Computação - UNICAMP

Marcelo Monte Karam – Graduado em Tecnologia em Segurança da Informação

André de Miranda – Aluno de Rede de Computadores - UNEB

Felipe Brant Sacarel – Bacharel em Ciência da Computação - UnB

#### Plano de Teste G1PT2

Tentativa não rastreável de fraude no resultado da votação

#### 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



Tribunal Superior Eleitoral  
PROTOCOLO  
4.300/2012  
13/03/2012 - 16:35  


*SSA*  
*DA*

## Plano de Teste do Sistema Eletrônico de Votação

### 1 Informações gerais

Título do plano de teste	<i>Tentativa não rastreável de fraude no resultado de votação</i>
Instituição proponente (se aplicável)	
Responsável	nome: <i>Diego de Freitas Aranha (Coordenador do Grupo 1)</i> e-mail: <i>dfaranha@cic.unb.br</i> telefone (do autor ou responsável): <i>(61) 9280-8555</i>
Sistemas afetados	<b>Software:</b> <i>Software de votação usado nas seções eleitorais.</i>  <b>Hardware:</b> <input type="checkbox"/> Microterminal <input type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input checked="" type="checkbox"/> Mídias  <b>Procedimentos:</b> <input type="checkbox"/> Carga da urna <input type="checkbox"/> Votação
Duração estimada do teste (em minutos)	<i>15 minutos</i>
Extensão do ataque	<input type="checkbox"/> Urna ou seção eleitoral <input type="checkbox"/> Local de votação <input checked="" type="checkbox"/> Zona eleitoral <input type="checkbox"/> Município <input type="checkbox"/> Unidade da Federação <input type="checkbox"/> País
Conhecimentos necessários	<i>Conhecimento superficial do código-fonte e do material produzido em uma votação (mídias e relatórios).</i>

#### Observações:

- O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
- Este plano deverá ter no máximo dez 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

*DA*



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

O proponente deverá apresentar um resumo geral e sucinto do teste informado.

O teste visa alterar o resultado de uma votação já encerrada, ou seja, alterar as escolhas dos eleitores registradas pela urna.

---

#### 3.2 Fundamentação

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

O teste objetiva verificar a hipótese de que é possível alterar o resultado de uma uma votação já encerrada exclusivamente a partir dos produtos da mesma.

---

#### 3.3 Precondições para o teste

Deverá ser apresentada lista de todas as informações, recursos materiais (inclusive software e respectivas versões) e recursos humanos necessários para a realização do teste por parte do proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto.

O teste requer apenas a utilização do software de votação para a realização de uma eleição simulada e de um software personalizado para o processamento dos arquivos armazenados na Mídia de Resultados.

---





### 3.4 Escopo - Superfície de Ataque

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo aqueles relacionados ao:

- Material (e.g. urna, mídias, lacres, etc.),
- Ambiente (e.g. condições de operação, sala, alimentação, etc.)
- Procedimento (e.g. verificação, emissão de zerésima, etc.)

*Haverá a necessidade de se manipular o estado contido na Mídia de Resultados.*

---

---

### 3.5 Janela de atuação simulada do atacante

O proponente deverá delinear precisamente a janela temporal de atuação do atacante, isto é, em quais instantes a atuação do atacante será necessária, correlacionando com as condições estabelecidas.

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

*O ataque requer apenas acesso à urna para a realização de uma votação simulada dentro dos procedimentos padronizados e acesso posterior aos materiais produzidos pela mesma.*

---

---

### 3.6 Pontos de intervenção

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção, para o teste de segurança no sistema eletrônico de votação, são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como *software* (e.g. programas assinados), *hardware* (e.g. extensão proprietária de BIOS), procedimentos (e.g. armazenamento de urnas), mídias (e.g. assinatura e criptografia do boletim de urna) e lacres.

*Será necessário superar a segurança oferecida pela assinatura digital realizada nos materiais provenientes de uma votação padronizada.*

---

---



### 3.7 Passos a serem realizados e material necessário

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, um exemplo de uma lista de passos:

1. Atacante tem acesso físico à mídia de votação.
2. Atacante, utilizando um computador portátil, lê a mídia de votação.
3. Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.
4. Fim

Os passos deverão ser detalhados. Os passos devem obrigatoriamente conter critérios de parada do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será trazido pelo investigador.

1. Atacante tem acesso aos produtos de uma votação (mídias e relatórios) (5 minutos);
2. Atacante, utilizando um computador portátil, processa a Mídia de Resultados utilizando um programa personalizado (5 minutos);
3. Atacante altera o resultado da eleição (5 minutos);
4. Fim (Total = 15 minutos).

Nenhum material será necessário para a realização dos testes além do que já é produzido em uma votação padronizada.

### 3.8 Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. Em especial, a descrição dos resultados esperados deve conter:

- Tipo do resultado esperado:
  - alteração do destino do voto;
  - quebra do sigilo do voto;
- Extensão do ataque:
  - urna ou seção eleitoral;
  - local de votação;
  - zona eleitoral;
  - município;
  - unidade da federação;
  - país.





O documento deverá ainda conter uma probabilidade esperada de sucesso do ataque, se possível fundamentada.

O ataque no resultado da votação tem abrangência de zona eleitoral e a probabilidade de sucesso deve cair com o aumento do número de votos que se deseja alterar.

### 3.9 Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, discorrer e fundamentar as condições e probabilidades de se:

- Não detectar o ataque;
- Detectar o ataque.

O ataque não deverá ser rastreável.

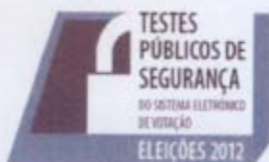
### 3.10 Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

A melhor solução vai depender do grau de sucesso do ataque.

BRASÍLIA, 13/03/2012

Diego de Freitas Aranha



## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G1PT2</b>	Coordenador:	Diego de Freitas Aranha	X
	Investigador 1:	Marcelo Monte Karam	X
	Investigador 2:	André de Miranda	X
	Investigador 3:	Felipe Brant Sacarel	X

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	17:33	Hora de Término:	-- : --
Resp. Acomp.:	Fausto Filho			Rubrica:	

Dados do Teste	
Título do teste:	Tentativa não rastreável de fraude no resultado da votação
Início do teste (Data/Hora):	-- / -- / -- -- : --
Termo do teste (Data/Hora):	-- / -- / -- -- : --
Critério de Parada:	Não há.

Relaxamento nos mecanismos e procedimentos de segurança
Não foi possível determinar quais mecanismos de segurança seriam relaxados, pois o teste não pôde ser realizado devido a escassez de tempo para tal.

Etapas Propostas para o Teste		
Etapa	Descrição	Status
1	Não foi possível determinar os passos necessários, pois o teste sequer chegou a ser realizado.	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
-- : --	Teste não realizado

Conclusões sobre o teste
Não existem conclusões sobre o teste proposto, frente ao fato de que o mesmo não foi realizado devido à falta de tempo para tal.

Considerações do grupo investigador
<p>Este ataque configuraria uma extensão do primeiro ensaio, realizado quando do desenvolvimento do plano de teste número um. O escopo desejado para tal ataque englobaria a interpretação do log armazenado na MR. Em virtude do tempo escasso para a realização do mesmo, tendo em vista a homologação do primeiro teste, optou-se pela não realização deste.</p> <p>Outro fator determinante para o sucesso deste, seria a interpretação de um log rotacional, fator este imprescindível para o sucesso do teste.</p> <p>Observou-se também a possibilidade de obtenção de dados gerais sobre a operação da Urna Eletrônica por intermédio de um arquivo de log armazenado na Flash Interna da Urna, supondo que este não contemple as mesmas características do arquivo encontrado na MR, ou seja, não é um log rotacional.</p>

Considerações do grupo de apoio
---------------------------------



Não foi possível realizar o teste supracitado, frente ao pouco tempo restante para o seu desenvolvimento. Maiores observações sobre o mesmo foram coletadas com a equipe de Investigadores, conforme segue relatado no item anterior.

#### Futuras Possibilidades

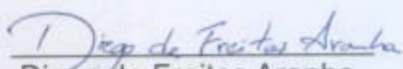
Não existem futuras possibilidades, pois o teste sequer chegou a ser realizado.

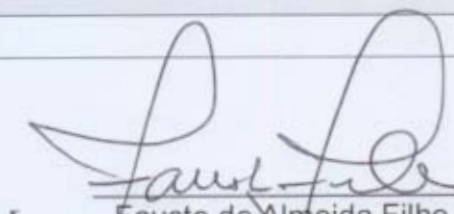
#### Alinhamento do PT

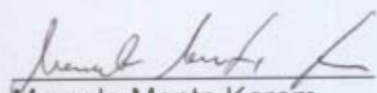
Não foi possível realizar nenhum alinhamento no plano de testes, pois o teste sequer chegou a ser realizado.

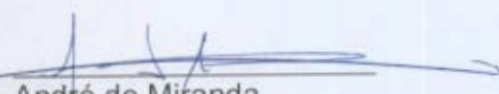
#### Informações Adicionais

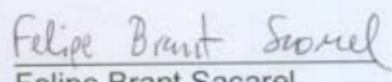
Não há.

  
Diego de Freitas Aranha

  
Fausto de Almeida Filho

  
Marcelo Monte Karam

  
André de Miranda

  
Felipe Brant Sacarel

