



# 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 G1PT1

Tentativa não rastreável de quebra de sigilo de 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

4.299/2012

13/03/2012 - 10:35



*[Handwritten signature]*

## Plano de Teste do Sistema Eletrônico de Votação

### 1 Informações gerais

Título do plano de teste	<i>Tentativa não rastreável de quebra de sigilo 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	
	<b>Resultado</b> <input type="checkbox"/> Aprovado <input type="checkbox"/> Aprovado com ressalvas <input type="checkbox"/> Reprovado	

*[Handwritten signature]*



### **3 Detalhamento do teste**

#### **3.1 Resumo do teste**

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

O teste visa quebrar o sigilo de uma votação já encerrada, ou seja, recuperar as escolhas do número máximo possível de eleitores naquela votação.

---

#### **3.2 Fundamentação**

O proponente deverá explicar, 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 recuperar os votos de uma eleição 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.)

*Não haverá necessidade de se alterar qualquer componente.*

---

---

### **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 precondições 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 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.

*Não será necessário superar nenhuma barreira de segurança, apenas garantir o acesso aos documentos e mídias produzidos por uma votação.*

---

---



### 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 recupera os votos depositados naquela 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 sigilo do voto tem abrangência de zona eleitoral e a probabilidade de sucesso deve cair com o aumento do número de votos que se deseja recuperar.

### 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 ainda encontra-se em estudo.

BRASÍLIA, 13/03/2012

Diego de Freitas Amanha



## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
	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:	20/03/2012	Hora de Início:	10:25
Resp. Acomp.:	Fausto de Almeida Filho	Hora de Término:	:
		Rubrica:	

Dados do Teste	
Título do teste:	Tentativa não rastreável de quebra de sigilo de votação
Início do teste (Data/Hora):	20/03/2012 10:25
Termino do teste (Data/Hora):	21/03/2012 16:10
Critério de Parada:	Finalização da execução do programa de análise e interpretação de sua saída para determinar se houve sucesso ou não.

Relaxamento nos mecanismos e procedimentos de segurança
Obter acesso à MR ou ao conteúdo desta após o término da eleição, logo após a remoção dos lacres da urna e a remoção das mídias, durante o momento que estas são entregues aos responsáveis pela apuração ou durante o trânsito desta para armazenamento, ou ainda durante o período no qual esta permanecer armazenada. O acesso aos documentos impressos pela urna facilita a execução do teste.

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Obter acesso à MR e/ou arquivos que nesta se encontram armazenados, quais serão transferidos para apuração.	OK
2	Executar um software construído para analisar a relação "eleitor x voto" baseado nos registros encontrados em tais arquivos.	OK
3	Repetir o passo 2 afim de se aprimorar o software de análise, até que se obtenha sucesso ou o método se mostre ineficaz.	OK

Procedimentos realizados durante o teste	
Hora	
10:25	- Boot do PC dos Investigadores utilizando a distribuição GNU/Linux Caine.
10:40	- Remoção dos lacres da MR/FV da UE2K9.
10:45	- Solicitação do envelope com as mídias, impressos e anotações do grupo.
10:50	- Solicitadas mídias de carga, votação e resultado.
11:10	- Grupo segue preparando os procedimentos para efetuação do teste.
11:15	- Início das preparações do teste, iniciando a carga da UE2K9.
11:20	- Início do processo de carga, com a data de 20/03/2012 e a hora 16:50.
11:25	- Término do processo de carga. Código de carga: 721.060.835.248.927.707.891.942 e Resumo de Correspondência: 981.942.

11:25	- Grupo encontra erro gramatical durante o boot da UE2K9, aonde lê-se "hot-plugue" ao invés de "hot-plug".
11:30	- Início dos testes pré-eleição da UE2K9.
11:31	- Emissão do relatório impresso dos testes.
11:35	- Emissão da zerézima.
11:35	- Início da votação.
11:35	<p>- Para efeito de conferência futura foram anotadas os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 1: V - Branco P - Branco</p> <p>Eleitor 2: V - 91001 P - 91</p> <p>Eleitor 3: V - 91102 P - 92</p> <p>Eleitor 4: V - 91003 P - 93</p> <p>Eleitor 5: V - 91004 P - 94</p> <p>Eleitor 6: V - 91005 P - 95</p>
11:40	- Finalização da eleição, emissão do BU e da justificativa.
11:41	- Remoção da MR.
11:41	- Remoção do lacre da USB frontal do PC dos Investigadores.
11:45	- Nova carga na UE2K9, com a data de 20/03/2012 e a hora 16:50.
11:50	- Término da carga da UE2K9, com o ID de carga 357.323.571.511.559.920.125.094 e Resumo de Correspondência 125.094.
11:51	- Início da análise dos arquivos na MR.
11:53	- Análise hexa dos arquivos presentes na MR.
11:58	- Preparação da UE2K9 para nova eleição. Realização dos testes preliminares e emissão da zerézima.
12:03	- Início de uma nova eleição em uma nova MR e FC.
12:03	<p>- Para efeito de conferência futura foram anotados os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 0049: V - Branco P - Branco</p> <p>Eleitor 0050: V - 91005 P - 95</p> <p>Eleitor 0051: V - 91004 P - 95</p>



	<p>Eleitor 0052: V - 91003 P - 93</p> <p>Eleitor 0053: V - 91002 P - 93</p> <p>Eleitor 0054: V - 91001 P - 91</p>
12:07	- Encerramento da eleição, emissão do BU e justificativa de Urna.
12:07	- Remoção da MR.
12:08	- Resumo de correspondência 127.094.
12:11	- Nova carga na UE2K9, com a data de 20/03/2012 e a hora 16:50.
12:15	- Cód. Carga: 417.929.742.117.014.004.237.147 e Resumo de Correspondência: 237.147.
12:20	- Almoço.
13:40	- Retorno do Almoço.
13:40	- Análise hexa dos arquivos presentes na MR.
14:33	- Início efetivo do plano de teste número 1.
14:35	- Requisição de cabine indevassável.
14:35	- Boot da urna com as seguintes mídias: FV: 543410227-6 MR: 600264970-4
14:40	- Emissão da zerézima e realização dos testes de software e hardware da UE2K9.
14:43	- Seleção dos eleitores e votos pela comissão de apoio.
14:45	- Início da votação.
14:59	<p>- Sessão carregada com apenas 180 eleitores válidos. Reiniciando seleção dos eleitores, considerando apenas a seleção dos primeiros 180 eleitores disponíveis na listagem. Para efeito de conferência futura foram anotados os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 0038: V - 92001 P - 00</p> <p>Eleitor 0001: V - 93005 P - 88</p> <p>Eleitor 0002: V - 93005 P - 55</p> <p>Eleitor 0003: V - 92001 P - 91</p> <p>Eleitor 0004: V - 92001 P - 91</p> <p>Eleitor 0005: V - 92001 P - 93</p>

*Diogo Almeida*

*Paulo*

*[Assinatura]*

*AA*

*[Assinatura]*

	<p>Eleitor 0006: V - 92001 P - 95</p> <p>Eleitor 0007: V - 93005 P - 91</p> <p>Eleitor 0008: V - 95001 P - 91</p> <p>Eleitor 0009: V - 95001 P - 94</p>
15:07	- Erro na mídia de resultado. Teste inválido.
15:10	- Nova carga na UE2K9. Serial da FC: 543007053-1.
15:12	- Início do processo de carga e testes de UE2K9, sendo a data definida como 20/03/2012 e a hora 16:59.
16:16	- Código de carga: 761.464.875.652.968.900.544.390.
15:16	- Resumo de correspondência 544.390.
15:17	- Mídias disponibilizadas para eleição: FV: 543008028-8 MR: 600264974-2
15:30	- Boot da UE2k9 para o teste 2.
15:37	<p>- Início da votação. Para efeito de conferência futura foram anotados os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 0050: V - 94004 P - 94</p> <p>Eleitor 0051: V - 94001 P - 91</p> <p>Eleitor 0052: V - 94002 P - 94</p> <p>Eleitor 0053: V - 93001 P - 95</p> <p>Eleitor 0054: V - 93001 P - 94</p> <p>Eleitor 0055: V - 95001 P - 93</p> <p>Eleitor 0056: V - 95002 P - 91</p> <p>Eleitor 0057: V - 91001</p>







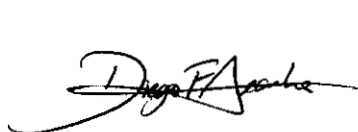

	<p>P - 92</p> <p>Eleitor 0058: V - 92003 P - 92</p> <p>Eleitor 0059: V - 00000 P - 00</p>
15:44	- Eleição finalizada, impressão dos documentos e mídias removidas.
15:45	- Urna desligada.
15:46	- Fornecidos para os Investigadores os produtos da eleição simulada.
15:50	- Análise dos dados da MR utilizando o software desenvolvido pelos Investigadores.
15:55	- Sucesso no teste. 10 de 10 votos recuperados da MR, sendo exibidos na tela por ordem cronológica de sufragação. Constanos nos dados exibidos pelo software a sequência dos eleitores, a opção do primeiro voto e a opção do segundo voto. Também é possível observar votos em branco e votos nulos, sendo que nestes não é possível conhecer os números fornecidos pelos eleitores.
16:07	- Nova carga na UE2K9, utilizando a FC de serial número 543007053-1.
16:07	- Data e hora da nova carga definidas como 20/03/2012 e 16:51.
16:15	- Final da carga da UE2K9, com código de identificação de carga 731.161.955.349.008.781.280.907 e resumo de correspondência 280.907.
16:16	- A mídia de resultado utilizadas durante esta eleição possuía o serial 600264975-9 e a flash de votação o serial 543001357-6.
16:18	- Boot da UE2K9.
16:22	- Testes de funcionalidade da UE2K9.
16:29	- Emissão da zerézima.
16:30	- Início da votação. A Equipe de Apoio irá escolher os votos dentre os eleitores elegidos para esta eleição e os investigadores irão computar os dados no equipamento.
16:44	<p>- Final da eleição. Para efeito de conferência futura foram anotados os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 0021: V - 93004 P - 93</p> <p>Eleitor 0033: V - 93001 P - 94</p> <p>Eleitor 0040: V - 92005 P - 92</p> <p>Eleitor 0048: V - 92001 P - 91</p> <p>Eleitor 0082: V - 93004 P - 93</p> <p>Eleitor 0090: V - 91004 P - 91</p> <p>Eleitor 0097:</p>

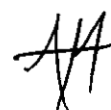






	<p>V - 92001 P - 92</p> <p>Eleitor 0105: V - 93001 P - 94</p> <p>Eleitor 0110: V - 91001 P - 91</p> <p>Eleitor 0134: V - 92002 P - 91</p> <p>Eleitor 0175: V - 95003 P - 91</p> <p>Eleitor 0230: V - 91002 P - 92</p> <p>Eleitor 0274: V - 92004 P - 92</p> <p>Eleitor 0326: V - 92005 P - 94</p> <p>Eleitor 0327: V - 93001 P - 95</p> <p>Eleitor 0340: V - 92004 P - 00</p>
16:47	- Hashes dos arquivos presentes na MR utilizada neste eleição foram calculados pela equipe de Apoio, e seguem anexos ao processo.
16:52	- Processamento dos arquivos da MR com o software desenvolvido pelos Investigadores.
16:57	- Sucesso no teste. todos os votos (16/16) foram recuperados da MR, sendo exibidos na tela por ordem cronológica de sufragação. Constanos nos dados exibidos pelo software a sequencia dos eleitores, a opção do primeiro voto e a opção do segundo voto. Também é possível observar votos em branco e votos nulos, sendo que já é possível observar a escolha dos números pelos votos nulos.
17:10	- Início de uma nova carga na UE2K9, utilizando a FC com o serial de número 543007053-1.
17:15	- Data e hora da carga definidas para 20/03/2012 às 16:50 horas.
17:20	- Para esta carga, foram fornecidos o Código de identificação de carga com o número 407.828.512.016.607.834.302.728 e o código de correspondência 302.728.
17:25	- Para esta eleição, utilizou-se a MR com serial de número 600264973-5 e a FV com serial de número 543008015-8.
17:30	- Início dos testes da urna.
17:35	- Início da eleição. Um membro da equipe de Apoio ficará sob o encargo de votar e anotar as escolhas, eleitor a eleitor e um segundo membro da equipe de Apoio ficará responsável por entrar com os dados dos eleitores.
17:43	- Problemas durante o processo de anotação dos votos. Votação Suspensa.




17:46	- Novo processo de carga na UE2K9, utilizando a flash de carga serial 543007053-1.
17:53	- Para esta eleição, serão utilizadas as mídia de votação com o serial de número 543007062-3 e a mídia de resultado com o serial de número 600264972-8.
18:05	- É iniciada um nova eleição, mantendo os padrões definidos para a última, aonde há participação ativa da comissão de apoio durante o processo de votação e identificação dos eleitores.
18:25	<p>- Eleição finalizada, documentos impressos e mídias removidas. Para efeito de conferência futura foram anotados os votos sufragados por cada eleitor, conforme segue:</p> <p>Eleitor 1: V - 93005 P - 95</p> <p>Eleitor 2: V - 92002 P - 93</p> <p>Eleitor 3: V - 95002 P - 93</p> <p>Eleitor 4: V - 94001 P - 95</p> <p>Eleitor 5: V - 95002 P - 91</p> <p>Eleitor 6: V - 94003 P - 92</p> <p>Eleitor 7: V - 93001 P - 94</p> <p>Eleitor 8: V - Branco P - 91</p> <p>Eleitor 9: V - 95004 P - Branco</p> <p>Eleitor 10: V - 94001 P - 94</p> <p>Eleitor 11: V - 92001 P - 77 (Nulo)</p> <p>Eleitor 12: V - 92001 P - 77 (Nulo)</p> <p>Eleitor 13: V - 91001 P - 95</p>



Diogo P. A. L.


Paul



AA



	<p>Eleitor 14: V - 93 (Legenda) P - 94</p> <p>Eleitor 15: V - 92004 P - 93</p> <p>Eleitor 16: V - 93004 P - Branco</p> <p>Eleitor 17: V - 93004 P - 94</p> <p>Eleitor 18: V - Branco P - 91</p> <p>Eleitor 19: V - 95 (Legenda) P - 93</p> <p>Eleitor 20: V - 91002 P - 94</p> <p>Eleitor 21: V - 92001 P - 93</p>
18:30	- Foram calculados os hashes dos arquivos presentes na MR por um membro da equipe de apoio.
18:34	- Execução do software desenvolvido pelos investigadores.
18:36	- Sucesso no teste. todos os votos (21/21) foram recuperados da MR, sendo exibidos na tela por ordem cronológica de sufragação. Constam nos dados exibidos pelo software a sequencia dos eleitores, a opção do primeiro voto e a opção do segundo voto. Também é possível observar votos em branco e votos nulos, sendo que já é possível observar a escolha dos números pelos votos nulos.
18:50	- Mídias, papéis e demais itens foram recolhidos e acondicionados em um envelope lacrado, assinado pela equipe de Apoio e pelo Investigador coordenador.
<b>21/03/2012 - Continuação do plano de teste</b>	
11:49	- Entrega do envelope com mídias, impressos e anotações.
11:55	- Início do processo de votação simulada, sugerida pela Sevin, afim de prover maior quantidade de dados para análise pelo software desenvolvido pelos investigadores. Durante esta eleição, foi utilizada uma sequencia de 478 eleitores, sendo que cada eleitor sufragou dois votos: um para vereador e outro para prefeito. O total máximo esperado para a seção carregada na UE para este teste era de 580 eleitores, respeitando assim a margem de abstinência real, observada pelo TSE.
12:00	- As mídias empregadas nesta eleição possuíam os seguintes números de série: FC: 543007053-1 FV: 543007059-3 MR: 600264963-6
12:00	- Boot da urna para a eleição simulada.
12:05	- Foram definidas a data e a hora da urna, conforme segue: 20/03/2012 - 15:30 h.
12:06	- A carga realizada na UE2K9 possuía o ID 347.222.451.410.341.546.724.706.




12:08	- Boot da UE2K9 seguido do processo de preparação para eleição.
12:16	- Impressão da zerésima, aonde se confirma da hora 15:43:04.
12:18	- Início da eleição.
14:10	- Término da eleição.
14:12	- Impressão da 1a. via do Boletim de Urna.
14:13	- Remoção da MR.
14:15	- Calculados os <i>hashes</i> dos arquivos presentes na MR.
14:30	- MR conectada ao terminal dos Investigadores, para análise de seu conteúdo e calibração do software de análise por eles desenvolvido.
14:31	- Decifração do programa para execução, qual se encontrava cifrado para salvaguarda de seu código fonte.
14:35	- Verificado o BU e zerésima para confirmação dos comparecimentos e eleitores habilitados para a sessão em questão.
14:35	- Executou o programa de análise, qual continha quatro parâmetros no ato de sua execução, sendo que o primeiro consistia em instante de tempo, sendo este adquirido à partir da zerésima. O intervalo de tempo fornecido se encontrava formatado no padrão MM/DD/HH:mm:ss. Logo após tal parâmetro, se encontravam o número de eleitores quais compareceram a eleição e o número total de eleitores previstos e caminho para o arquivo do RDV.
14:40	- O programa inicialmente obteve sucesso até o voto de número 275, porém encontrou erros nos vos subseqüentes, exigindo assim alterações em seu código fonte.
14:40	- Início da depuração do erro encontrado.
15:00	- Solucionado o problema, o programa de análise foi re-executado, produzindo assim a saída para apuração.
15:35	- Foi formada uma equipe de apuração, contendo um membro da equipe de Apoio e um funcionário do TSE, quais foram responsáveis por avaliar voto à voto, o grau de sucesso do programa de análise. Os membros da equipe de investigadores monitoraram o processo de maneira passiva.
15:35	- Foi iniciada uma apuração por amostragem, sendo que 25 votos foram escolhidos aleatoriamente afim de serem comparados com os dados fornecidos pelo programa de análise. À partir desta apuração, obteve-se 100% de sucesso nos dados analisados.
15:42	- Início da apuração voto à voto. Observou-se que o programa de análise foi capaz de recuperar 99,99% dos votos sufragados. A não recuperação de um único voto, no caso um voto para vereador, foi devida a um erro humano na entrada dos dados.
Em tempo	O investigador Coordenador, responsável pela execução do software de análise dos produtos da eleição, esteve ausente da sala durante o período de votação simulada, afim de impedir a comunicação entre os membros da equipe.

#### Conclusões sobre o teste

Inicialmente, o teste obteve sucesso absoluto em eleições simuladas com até 21 eleitores, escolhidos aleatoriamente. Em seguida, sugeriu-se um cenário mais amplo, o qual compreendia uma eleição baseada em dados reais. O teste recuperou 99,99% desta eleição simulada com 580 eleitores possíveis, com o nível de comparecimento de 475 eleitores, estando este complacente com a média de abstenção observada pelo TSE nas eleições de 2010.

O sucesso do teste depende exclusivamente de um erro de projeto no arquivo de Registro dos Votos (RDV). Este arquivo é organizado como uma tabela que permite escritas em qualquer posição e o número total de posições corresponde ao número de eleitores registrados na seção eleitoral. A cada escrita de um voto no arquivo, uma nova posição é selecionada aleatoriamente, com o objetivo de desvincular a ordem de votação e a ordem de armazenamento.

Entretanto, a sequência de escrita no RDV é determinística e pode ser derivada independentemente a partir dos produtos públicos de uma eleição. De posse destes e da ordem dos eleitores votantes, é possível violar o sigilo do voto. O procedimento executado pelo programa de análise consiste em derivar esta sequência alternativa de posições em que os votos foram escritos no RDV e recuperá-los posteriormente.







Caso não seja possível obter os produtos públicos, é possível percorrer um espaço pequeno de diferentes valores em busca da sequência exata de escrita observada no RDV. Determinado este valor, o teste pode prosseguir como descrito no parágrafo anterior.

#### **Considerações do grupo investigador**

A razão para a vulnerabilidade é a utilização de um gerador de números pseudo-aleatórios de baixa qualidade. O RDV é um componente crítico para assegurar o sigilo do voto e sua sequência de escrita precisa ser obtida a partir de um gerador de qualidade criptográfica. Como o teste executa apenas leitura dos produtos de uma votação, nenhum rastro é deixado.

Recomenda-se corrigir a vulnerabilidade a partir da utilização de um gerador de números pseudo-aleatórios de qualidade criptográfica. Idealmente, este gerador deve ser implementado em *hardware* e sua qualidade deve depender de um efeito físico bem estudado. Caso não seja possível adotar esta solução para todos os equipamentos, sugere-se utilizar o gerador nativo do sistema operacional GNU/Linux acessado a partir do arquivo `/dev/random`. Entretanto, a qualidade desse gerador depende da entropia recolhida a partir de eventos em nível de sistema operacional. Como o ambiente de execução da urna eletrônica é controlado e, consequentemente, previsível, é fundamental determinar previamente se a solução atinge o seu propósito. Outro aspecto a se analisar é se o gerador nativo produz banda suficiente para utilização nesse cenário, visto que seu meio de acesso é bloqueante, o que pode interferir com a funcionalidade da urna. Em último caso, sugere-se recorrer ao gerador nativo implementado a partir do arquivo `/dev/urandom`, mas cabe a consideração de que este último não alcança qualidade criptográfica, ainda que seja superior ao utilizado atualmente.

#### **Considerações do grupo de apoio**

Frente aos fatos observados durante a execução do plano de teste, é importante apresentar as seguintes considerações:

**Sobre a execução do plano de teste:** A execução do plano de teste se deu conforme o esperado, sendo que todas as etapas sugeridas pelos proponentes foram executadas. Não foi observada nenhuma modificação nas atividades propostas, sendo estas realizadas conforme o descrito no plano de teste.

**Sobre o tempo de execução do plano de teste:** Segundo o documento submetido pelos Investigadores, a duração estimada do teste era de quinze minutos, sendo que na verdade o tempo para construção dos mecanismos necessários para tal ocorreria num período de tempo maior, de vinte e seis minutos. Mesmo desconsiderando o tempo necessário para realização das eleições e a conferência dos resultados, o tempo empregado no desenvolvimento do programa para recuperação dos votos foi superior ao sugerido pelos Investigadores. Tal característica não compromete o resultado alcançado pelo grupo, frente ao fato do sucesso ao fim do desenvolvimento da aplicação.

**Sobre a aplicabilidade prática do produto do teste:** Para que o grupo fosse capaz de desenvolver o programa responsável por recuperar a ordenação dos votos sufragados em uma MR, foram necessárias diversas interações com os produtos de diferentes eleições conforme relatado no acompanhamento dos fatos. É importante salientar que tais eleições foram realizadas sequencialmente, contemplando desde o processo de carga, votação e fechamento da sessão, sendo que tais características fogem ao processo comum de um pleito.

Sabe-se que tais interações forneceram subsídios para a concepção da ideia, formulação de um programa inicial e aperfeiçoamento da solução desenvolvida. Deste modo, vale salientar que se tratando de um ambiente real, acredita-se, que um atacante não disporia com facilidade de tais subsídios.

Faz-se importante saber que o código fonte em desenvolvimento para as eleições de 2012 não está amplamente distribuído ao público, o que dificultaria tentativas de desenvolvimento de um algoritmo similar ao empregado pelos investigadores em seu programa.

Outro ponto chave para o sucesso do ataque é o conhecimento da ordem dos eleitores participantes de cada sessão, de modo a apontar as opções de cada eleitor. Para tal, é necessário que um terceiro esteja anotando a ordem de entrada e saída dos eleitores da sessão eleitoral, sendo que este pode ser um terceiro ou até mesmo um dos integrantes da mesa de votação.





**Sobre a rastreabilidade do teste:** Conforme relatado pelos Investigadores, de fato não é possível observar qualquer alteração nos arquivos submetidos à análise pelo programa por estes desenvolvido. Os *hashes* foram calculados quando do término da eleição simulada e após a execução do programa, de modo a permitir a comparação dos mesmos. Assim, os *hashes* foram comparados, um à um, conferindo 100% de integridade aos arquivos após a execução do programa.

**Sobre a facilidade de obtenção dos produtos de uma eleição:** É preciso saber que alguns dos produtos necessários para realização deste teste estarão disponíveis ao público, porém, serão condicionados a solicitações formais, que deverão ser submetidas às regionais, de modo que haverá registros de quais informações foram cedidas a qual solicitante.

Além disso, faz-se importante salientar que para o desenvolvimento de suas hipóteses o grupo investigador necessitou realizar um conjunto de eleições parametrizadas.

**Sobre as recomendações realizadas:** Entende-se que as recomendações realizadas pelos Investigadores deverão ser alvo de maiores estudos a fim de aferir a sua empregabilidade.

#### **Futuras Possibilidades**

- Foram discutidas diversas soluções, porém todas se mostraram pouco práticas ou mais difíceis de implementar do que a sugerida previamente.
- Não é possível afirmar se através dos procedimentos realizados seria possível obter outros tipos de dados, frente ao curto período de tempo disponível para a realização de maiores testes.

#### **Alinhamento do PT**

**Impacto do ataque:** País

**Número de Pontos de Intervenção:** São necessários dois pontos de intervenção, conforme segue:

- 1 – Ordem dos votantes
- 2 – Arquivo RDV

#### **Informações Adicionais**

- Segundo um dos membros do Grupo, a presença e a intervenção constante por parte de elementos externos à equipe de apoio e os grupos de investigadores, acabou por interferir no bom andamento dos testes.
- A duração dos testes deveria ser otimizada, podendo contar com em média uma semana (cinco dias úteis) para realização dos mesmos.
- O acesso ao código-fonte foi melhorado, mas segundo os membros do grupo, este ainda é carente. A sugestão é que sejam disponibilizadas estações individuais para cada um dos grupos inscritos, afim de otimizar o tempo para cada análise.

  
Diego de Freitas Aranha

  
Marcelo Monte Karam

  
André de Miranda

  
Felipe Brant Scarel

  
Fausto de Almeida Filho

