



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012  
Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 05

Representando a Universidade Federal de Uberlândia - UFU

Marcelo Rodrigues de Sousa – Doutor em Engenharia Elétrica e Computação – UFU

Kil Jin Brandini Park – Pós-doutorado em Ciência da Computação – CTI Renato Archer

Otávio Augusto Araújo da Silva – Graduado em Ciência da Computação - UFU

#### Plano de Teste G5PT1

UFO-FACOM-TEFSEV: Modificação do boot da urna

#### 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	UFU-FACOM-TEPSEV
Instituição proponente (se aplicável)	UNIVERSIDADE FEDERAL DE UBERLÂNDIA/FACULDADE DE COMPUTAÇÃO
Responsável	nome: MARCELO RODRIGUES DE SOUSA e-mail: marcelo@facom.ufu.br ou marcelo@ufu.br telefone (do autor ou responsável): (34)9958-5050 (Celular) ou (34)3239-4478 (UFU)
Sistemas afetados	<b>Software:</b> <input checked="" type="checkbox"/> Software de votação usado nas seções eleitorais.  <b>Hardware:</b> <input type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input checked="" type="checkbox"/> Lances <input checked="" type="checkbox"/> Mídias  <b>Procedimentos:</b> <input checked="" type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	5 horas e 50 minutos (todos os 4 ataques)
Extensão do ataque	<input checked="" 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	Conhecimentos profundos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.

#### 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



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

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

Serão realizados 4 (quatro) testes:

##### **A. Modificação do boot da urna**

*Descrição:*

*Tentativa de alterar parâmetros de boot da urna eletrônica de maneira a comprometer seu funcionamento.*

*Este teste será constituído de duas metodologias distintas. Na primeira, teste de modificação dos parâmetros de boot da urna para que esta não funcione conforme o previsto. Na segunda, teste de alteração dos parâmetros de boot da urna para que esta force o boot a partir de uma mídia distinta da mídia de carga, com o intuito de sobrepôr o sistema de verificação e forçar a carga de um sistema operacional não autorizado.*

*Tipo de Ataque: Falha*

*Duração do teste: 30 minutos.*

*Pontos de intervenção: rompimento dos lacres e alteração da mídia de carga.*

*Extensão do ataque: Urna Eletrônica.*

##### **B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Descrição:*

*Teste de recuperação de dados da memória volátil da urna, tanto para modificação de dados relativos a votação quanto para tentativa de recuperação de dados utilizados para cifragem do sistema operacional e assinatura dos programas internos.*

*Tipo de Ataque: Falha*

*Duração do teste: 30 minutos.*

*Pontos de intervenção: rompimento dos lacres e alteração da mídia de carga.*

*Extensão do ataque: Urna Eletrônica.*

##### **C. Tentativa de comprometimento do MSD através da interface JTAG**

*Descrição:*

*Tentativa de conectar equipamento na interface JTAG da placa da urna, para comprometimento do MSD.*

*Tipo de Ataque: Falha*

*Duração do teste: 4 horas.*

*Pontos de intervenção: rompimento dos lacres.*

*Extensão do ataque: Urna Eletrônica.*

##### **D. Quebra do sigilo do voto eletrônico**

*Descrição:*

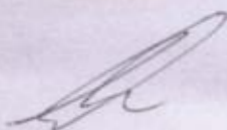
*Demonstração da possibilidade de uma pessoa determinar se um eleitor votou ou não em um determinado candidato usando a urna eletrônica, fazendo uma comparação com o processo de votação manual.*

*Tipo de Ataque: Fraude.*

*Duração do teste: 10 minutos.*

*Pontos de intervenção: 1 ponto (risco da urna).*

*Extensão do ataque: Brasil.*



### 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.

*A fundamentação dar-se-á para cada teste separadamente:*

#### A. Modificação do boot da urna

*Tentativa de alterar parâmetros de boot da urna eletrônica de maneira a comprometer seu funcionamento.*

*Este teste será constituído de duas metodologias distintas. Na primeira, efetuaremos tentativas de modificação dos parâmetros de boot da urna para que esta não funcione conforme o previsto. Na segunda, tentaremos alterar os parâmetros de boot da urna para que esta funcione a partir de uma mídia distinta da mídia de carga, com o intuito de subverter o sistema de verificação e forçar a carga de um sistema operacional não assinado. Considera-se que o atacante tem acesso hipotético a uma urna eletrônica, que pode ter sido substituída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso neste teste.*

#### B. Tentativa de recuperação de dados da memória volátil do equipamento

*Tentativa de recuperação de dados da memória volátil da urna, tanto para modificação de dados relativos à votação quanto para tentativa de recuperação de chaves utilizadas para criptografia do sistema operacional e assinatura dos programas internos.*

*Para tanto, a metodologia consiste em abrir a urna eletrônica, desligá-la durante uma operação, rapidamente barrifar sobre o pente de memória uma solução resfriante, retirar o pente, conectá-lo a um outro equipamento preparado para bootar com um software que copie o conteúdo da memória para uma mídia externa (USB). É necessário o acesso físico a uma urna eletrônica, considera-se que o atacante tem acesso hipotético a uma urna eletrônica, que pode ter sido substituída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso neste teste.*

#### C. Tentativa de comprometimento do MSD através da interface JTAG

*Tentativa de conectar equipamento na interface JTAG da placa da urna, para comprometimento do MSD. Considera-se que o atacante tem acesso hipotético a uma urna eletrônica, que pode ter sido substituída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso neste teste. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso neste teste.*

#### D. Quebra do sigilo do voto eletrônico

*Demonstração da possibilidade de uma pessoa determinar se um eleitor votou ou não em um determinado candidato usando a urna eletrônica, fazendo uma comparação com o processo de votação manual. Será feita uma análise de todo processo de votação desde a carga da urna até a sua apuração. Esse teste usa a criatividade como principal arma de ataque ao sistema de votação.*





### 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.

*Para cada teste proposto são necessários:*

#### A. Modificação do boot da urna

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB. Alteração da mídia de carga.*

*Equipamentos necessários:*

*Teclado externo via USB.*

*Memória USB (pendrive).*

*Cartão de memória de carga da urna.*

*Dois conversores USB/RJ232 e um adaptador db9 fêmea.*

*Conhecimentos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.*

#### B. Tentativa de recuperação de dados da memória volátil do equipamento

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB.*

*Equipamentos necessários:*

*Spray de elemento refrigerante/congelante (nitrogênio) não dermatológico, como:*

*"Multi-Purpose Freeze Spray"*

*"Spray CONGELANTE IMPLANTEC"*

*"MAX Profissional 7777 Blow Off Freeze Spray Electronic Component Cooler"*

*"SPRAY CONGELANTE GELO DUE-CT"*

*"Spray Congelante Ixi"*

*"Spray Congelante de Ação Rápida CS68"*

*Memória USB (pendrive) de 8Gb para configuração do software de extração.*

*Notebook compatível com memória de mesmo tipo utilizada na urna eletrônica (DDR2), capaz de boot pela interface USB.*

*Conhecimentos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.*

#### C. Tentativa de comprometimento do MSD através da interface JTAG

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB.*

*Equipamentos necessários:*

*Interface JTAG macho a ser colada nos conectores JTAG existentes na placa da urna, e fita isolante, a fim de evitar qualquer ruído.*

*Cabo JTAG – USB a ser utilizado para conexão entre um computador e a urna, dentre os seguintes: ULINK ME, ULINK2, ULINKPro, J-Link Lite, J-Link LPC Edition, J-Link ARM.*

*Mídia ROM com Keil ARM Evaluation Kit disponível em:*  
<http://www.keil.com/demo/eval/arm.htm>





#### *D. Quebra do sigilo do voto eletrônico*

*Não há pré-condições.*

### **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 zerêsima, etc.)

*Para cada teste:*

#### *A. Modificação do boot da urna*

*Rompimento dos lacres da urna eletrônica.*

*Alteração da mídia de carga.*

#### *B. Tentativa de recuperação de dados da memória volátil do equipamento*

*Rompimento dos lacres da urna eletrônica.*

#### *C. Tentativa de comprometimento do MSD através da interface JTAG*

*Rompimento dos lacres da urna eletrônica.*

#### *D. Quebra do sigilo do voto eletrônico*

*Não há modificações nas urnas eletrônicas.*

### **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.

*Para cada teste:*

#### *A. Modificação do boot da urna*

*Acesso às mídias de carga das urnas anteriormente ao período de votação.*

#### *B. Tentativa de recuperação de dados da memória volátil do equipamento*

*Acesso à urna eletrônica antes ou após o pleito.*

#### *C. Tentativa de comprometimento do MSD através da interface JTAG*

*Acesso à urna eletrônica antes do pleito.*

#### *D. Quebra do sigilo do voto eletrônico*

*A atuação se dá durante o processo eleitoral (dia de votação).*



### 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.

*Para cada teste:*

**A. Modificação do boot da urna**

*rompimento dos lacres e alteração da mídia de carga*

**B. Tentativa de recuperação de dados da memória volátil do equipamento**

*rompimento dos lacres*

**C. Tentativa de comprometimento do MSD através da interface JTAG**

*rompimento dos lacres e alteração da mídia de carga*

**D. Quebra do sigilo do voto eletrônico**

*Uso do display da urna eletrônica.*

### 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.

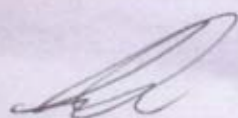
O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será trazido pelo investigador.

*Para cada teste:*

**A. Modificação do boot da urna**

*Lista de passos:*

1. Atacante tem acesso físico à urna e à mídia de carga.
2. Atacante, utilizando um computador portátil, lê e altera a mídia de carga.



3. Com a mídia alterada dá-se carga à urna com o processo de boot modificado.
4. Fim

#### **B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Lista de passos:*

1. Atacante tem acesso físico à urna eletrônica.
2. Atacante desmonta a urna, retirando seus lacres.
3. Atacante inicializa a urna e usa o spray em momento oportuno.
4. Atacante retira a memória RAM da urna e a conecta em um computador portátil.
5. Atacante faz dump da memória e busca dados espalhados.
6. Fim

#### **C. Tentativa de comprometimento do MSD através da interface JTAG**

*Lista de passos:*

1. Atacante tem acesso físico à urna eletrônica.
2. Atacante desmonta a urna, retirando seus lacres.
3. Atacante conecta o JTAG ou o cabo serial na placa-mãe da urna.
4. Atacante executa um software para debug ou reprogramação da urna usando um computador portátil.
5. Atacante inicializa a urna.
6. Atacante aguarda a urna entrar em processo de debug ou reprograma a própria urna.
7. Fim

#### **D. Quebra do sigilo do voto eletrônico**

*O processo se dá no dia da votação através de ações criminais eleitorais.*

### **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.

*Resultados esperados dos testes:*

#### **Modificação do boot da urna**

*Possibilidade de controle do kernel da urna eletrônica, fazendo-a comportar-se maliciosamente.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrônica.*







Taxa de sucesso esperada: 99%

#### ***Tentativa de recuperação de dados da memória volátil do equipamento***

*Possibilidade de extração das chaves criptográficas da urna para uso posterior.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrónica*

*Taxa de sucesso esperada: 70%*

#### ***Tentativa de comprometimento do MSD através da interface JTAG***

*Possibilidade de extração das chaves criptográficas da urna para uso posterior ou reprogramação da urna electrónica.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrónica*

*Taxa de sucesso esperada: 40%*

#### ***Quebra do sigilo do voto electrónico***

*Possibilidade de quebra do sigilo do voto de um eleitor, dessa forma pode-se verificar se um eleitor votou ou não em uma determinado candidato.*

*Tipo de Ataque: Fraude*

*Extensão do ataque: Brasil*

*Taxa de sucesso esperada: 99%*

### **3.9 Rastreabilidade**

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

- Não detectar o ataque;
- Detectar o ataque.

*Resultados esperados de rastreabilidade:*

#### ***Modificação do boot da urna***

*Probabilidade de rastreamento: é possível detectar o ataque através de processos de segurança, basta auditar a mídia de carga. Há rompimento dos lacres.*

#### ***Tentativa de recuperação de dados da memória volátil do equipamento***

*Probabilidade de rastreamento: é possível verificar o rompimento dos lacres, mas não é possível detectar se as chaves foram descobertas.*

#### ***Tentativa de comprometimento do MSD através da interface JTAG***

*Probabilidade de rastreamento: é possível verificar o rompimento dos lacres, mas não é possível detectar se as chaves foram descobertas. No caso de reprogramação da urna, esta modificação é detectável através de auditoria.*

#### ***Quebra do sigilo do voto electrónico***

*Não é possível detectar o ataque, a menos de denúncia prévia.*



#### ***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.

*Nas testes abaixo são soluções:*

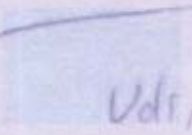
#### ***Modificação do boot da urna***

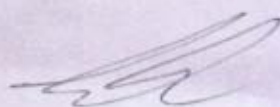
*Todos os parâmetros do boot serem built-in no kernel, e o kernel não aceitar parâmetros de boot.*

#### ***Tentativa de comprometimento do MSD através da interface JTAG***

*Tanto a porta serial e JTAG serem resinadas.*

*As outras soluções quanto possíveis serão apresentadas após o início dos testes.*

*H. WJ*  *Vdr, 13/03/2012*







## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G5PT1</b>	Coordenador:	Marcelo Rodrigues de Sousa	
	Investigador 1:	Kil Jin Brandini Park	
	Investigador 2:	Otávio Augusto Araújo Silva	

Informações do Acompanhamento					
Data:	20/03/2012	Hora de Início:	10:20	Hora de Término:	10:45
Resp. Acomp.:	Marco Constantino			Rubrica:	

Dados do Teste			
Titulo do teste:	UFO-FACOM-TEFSEV: Modificação do boot da urna		
Início do teste (Data/Hora):	20/03/2012		10:20
Termino do teste (Data/Hora):	21/03/2012		10:45
Criterio de Parada:			

Relaxamento nos mecanismos e procedimentos de segurança	
O lacre do slot da flash de carga foi rompido para que fosse possível o acesso a flash de carga.	

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Todo o teste ocorreu conforme relatado no plano de testes	
2		
3		
4		
5		
6		
7		
8		
9		
10		

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste

	<p>Solicitação das mídias usadas no pré-teste</p> <p>Abertura dos dados contidos nessas mídias no computador do investigador, verificou-se que seria necessário a restauração dos dados originais na flash, o procedimento foi feito e em seguida abriu-se os dados no editor Hexa.</p>
10:55	<p>Modificações são realizadas nos arquivos através de inserção/deleção de caracteres Hexa, dessa maneira ocorrem mudanças de estrutura no arquivo adicionando informações ou subtraindo-as.</p> <p>Após a execução das modificações - que na sua grande maioria não passaram de mudanças de valores Hexa os arquivos foram salvos na flash de carga(FC).</p>
11:03	<p>Para o devido acesso à FC contida na urna e sua troca pela FC modificada pelo investigador, o lacre que promove a inviolabilidade do slot onde se armazena a FC foi rompido para que o investigador pudesse efetuar a troca. Interessante notar que foi arguido ao investigador como ele procederia diante de outros fatores que são premissas anteriores para se conseguir acesso a urna e consequentemente à FC e, consequentemente, a volta da FC modificada à Urna.</p> <p>O investigador contextualizou seu ataque informando que a urna teria sido furtada do galpão de armazenamento logo após a carga oficial anterior a eleição, em localidades rurais ou ribeirinhas, onde a vigília das urnas é precária em comparação a outras áreas do país. Após feita as modificações na FC ele seria devolvida antes do início das votações. Para tal o atacante informou que seria necessário a participação de terceiros, uma vez que o acesso as áreas de armazenamento da urna são controladas por agentes de segurança. Mesmo após todas essas barreiras vencidas ainda seria necessário que o atacante tivesse condições de não deixar vestígios de rompimento do lacre do slot da FC.</p>
11:05	<p>Após contextualizarmos o ataque foi inserido a FC modificada na urna.</p> <p>Urna ligada, o sistema carregou, com um parâmetro de boot do kernel alterado, com uma singela modificação: O pinguim que antes aparecia no boot inicial agora estava ausente devido modificação no parametro de inicialização da VGA da urna. Entretanto após carregar todo do Sistema Operacional(SO) a urna travava ao carregar o aplicativo de votação, e apresentava o seguinte erro:</p> <p>"SDL_ScreenPrint no Availabe Video Device".</p>
11:10	<p>Urna reiniciada</p> <p>O investigador passou alguns minutos olhando a tela de inicialização modificada. Como ela não apresenta mais a imagem do pinguim, ficou mais fácil de se observar tudo que ela carrega durante o processo de inicialização. O investigador procurava um "Mount Device Point" pronto no boot para inserção de arquivos.</p>
11:15	<p>Dispositivo montado no PC do investigador - Flash de carga. Comando chdisk executado para listar as partições e observar como elas estavam distribuídas dentro do FC. O objetivo do investigador era inserir um binário produzido por ele dentro da FC e efetuar a chamada desse binário dentro do Kernel.</p> <p>Ele produziu um pequeno script para teste e inseriu o arquivo dentro da FC da urna, após feito isso, foi novamente inserida na urna a FC e tentado o boot com arquivo modificado.</p> <p>Após a inicialização de parte do, SO a urna travou com o seguinte erro:</p> <p>"SDL_ScreenPrint no Availabe Video Device".</p> <p>Sendo assim, o investigador retornou os valores anteriores de boot do kernel na FC, utilizando o editor Hexa e novamente com o arquivo alheio ao sistema dentro da FC ele tentou o boot.</p> <p>Nessa tentativa foi observado o correto carregamento da urna eletrônica, não houve travamentos. Todo o processo de carga</p>





	<p>da urna ocorreu corretamente, e ao fim o processo a urna reiniciou-se, um comportamento esperado ao fim da carga.</p> <p>O investigador questionou se o arquivo dele havia sido copiado para dentro da urna, o que prontamente foi respondido pela equipe de apoio explicando o funcionamento do SCUE e indicando ao investigador que retirasse a flash interna(FI) para observar quais arquivos lá se encontravam, o investigador não achou necessário tal procedimento.</p>
12:00	<p>Investigador novamente utilizando o editor Hexa fez uma tentativa de modificação visando aportar o init do boot para o arquivo b, criado por ele, que fora colocado na partição, root para boot, da FC.</p> <p>O investigador efetuou mais algumas modificações hexa e ao iniciar a urna o erro "SDL_ScreenPrint no Availabe Video Device" novamente apareceu.</p>
14:30	<p>Foi solicitado pelo investigador se seria possível adentrar o recinto com CD-R contendo alguns arquivos que seriam utilizados no teste. A solicitação foi atendida e o investigador entrou no recinto com um CD-R contendo arquivos, logo após a inserção do CD no PC do investigador ele extraiu alguns dados do CD e observou que havia um arquivo corrompido.</p>
14:53	<p>Solicitou download do arquivo que se encontrava corrompido no CD: Kernel 2.6.16</p>
15:05	<p>Lacre frontal do PC do investigador foi rompido devido mal funcionamento da USB, assim como o lacre traseiro rompido também para testes de USB com o leitor de mídias.</p>
16:45	<p>Foi gravado um CD-R com as informações solicitadas por download e em seguida arquivos extraídos do CD para o desktop. Feita a compilação do Kernel, foi montado um initramfs para o kernel 2.6.16, utilizando o gcc-4.1, afim de se inicializar a urna na esperança do init contido no initramfs ser executado antes do initje.</p> <p>Novamente o investigador abriu os arquivos no editor Hexa e efetuou mudanças, para o kernel utilizar o initramfs, armazenado na partição root para o boot da FC, copiou todas essas informações para dentro da mídia de carga e inseriu na urna para outra tentativa de boot. A urna foi inicializada normalmente, indicando que o kernel aparentemente ignorou o initramfs.</p> <p>Uma nova tentativa fora feita, agora apontando o init para um arquivo não oficial, adicionado por ele, na partição root para boot da FC, dessa o kernel executou o binário não oficial, porém houve um erro na função execve, da libc :</p> <p>"Kernel Panic - execve(-1)"</p> <p>O investigador deduziu que fora um erro gerado pelo loader elf no kernel, já que o arquivo oficial não possui nenhuma assinatura, por tanto tentou-se a execução pelo kernel de um arquivo assinado e diferente do initje .</p> <p>Foi utilizado um arquivo contido no diretório /uenux/bin/smt como o init, pois o mesmo provavelmente seria assinado, e conteria a mesma em algum campo do formato ELF.</p> <p>A urna foi reinicializada e o boot ocorreu até a execução do suposto init.</p> <p>O arquivo foi executado pelo kernel sem problemas, porém como esse arquivo não é um init para System V, o mesmo terminou, ou interrompeu sua própria execução, provavelmente pela chamada de bibliotecas ainda não presentes no ambiente, levando o kernel ao panic, pelo término prematuro do init, travando na seguinte mensagem de erro:</p> <p>"Kernel Panic - attempted to kill init!"</p> <p>Por fim testou-se outros parâmetros de kernel, como trocar a fonte de clock, desabilitar interfaces de hardware, forçar o kernel a não randomizar o mapeamento de memória ou forçar o uso de apenas algumas regiões de memórias. Como resultado desses parâmetros obteve-se alguns erros:</p> <p>Ao desabilitar todas interfaces USB: Erro de comunicação com o MSD!</p> <p>Ao desabilitar o APIC,HPET (noapic , hpet=off)</p> <p>MSD levou de 15 a 20 segundos a mais para desligar a urna quando não recebia os</p>







#### Conclusões sobre o teste

Após os testes, observou as diversas possibilidades de manipulação dos parâmetros de kernel para o boot, apesar de nenhuma das tentativas terem levados a um maior acesso ao sistema operacional, como a inserção de comandos arbitrários ou a execução suscetível de arquivos alheios, é possível por exemplo a troca do init, o uso de um initramfs melhor preparado, desabilitar interfaces de hardware, como USB, SCSI, ou manipular a fonte de clock, desabilitar o HPET, entre outros.

Apesar de não conseguirmos alterar resultados de votações, a possibilidade de alteração de parâmetros de inicialização abre brechas para tentativas de outros ataques. Nesse contexto, ataques baseados em dump de memória são facilitados ao utilizar parâmetros que indiquem o uso de trechos específicos de memória sem a utilização de randomização, e a redução das áreas de memórias que o kernel pode mapear reduz a presença de dados "lixo" possivelmente presentes nos dumps. Pois esta redução do espaço de endereçamento e conjunto com a não randomização do mapeamento da memória torna o processo de alocação e uso de memória pelo kernel uma sucessão de endereços altamente próximos incrementais.

Esta concepção da redução do mapeamento não randômico foi utilizado como uma premissa de aumento de sucesso em um segundo teste feito na urna

Por fim, foi concluído que talvez com um maior tempo de testes e de tentativas, talvez fosse possível manipular o kernel a agir de maneira a facilitar ataques mais promissores e possivelmente extrair mais informações de memória ou de arquivos lidos pelo kernel.

#### Considerações do grupo investigador

#### Considerações do grupo de apoio

Todo o teste ocorreu como relatado no plano de testes, interessante notar que as modificações nos parâmetros do kernel para forçar o um boot modificado são extremamente válidas, uma vez que é possível sumir com o pinguim que aparece na inicialização ou mesmo forçar algum outro tipo de parâmetro que favoreça ataques mais sofisticados.



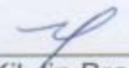

Futuras Possibilidades


Alinhamento do PT
Todo o teste transcorreu de acordo com o relatado no plano de testes.

Informações Adicionais

\_\_\_\_\_  
Marcelo Rodrigues de Sousa

  
\_\_\_\_\_  
Marco Constantino

  
\_\_\_\_\_  
Kil Jin Brandini Park

  
\_\_\_\_\_  
Otávio Augusto Araújo Silva

