Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

Relatório dos resultados da realização dos Testes Públicos

Investigador Individual 3

Representando a Marinha do Brasil

Suzana Brandt Dias – Graduada em Processamento de Dados – Universidade Estácio de Sá
Encarregada da Divisão de Operações de Guerra Cibernética do Centro de Tecnologia da Informção da Marinha

Plano de Teste I3PT1

Comprometimento da transferência dos resultados obtidos nas urnas para o servidor do TRE/TSE

Conteúdo deste relatório

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

INV-3

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título do plano de teste	Comprometimento da transferência dos resultados obtidos nas urnas para o servidor do TRE/TSE
Instituição proponente (se aplicável)	Marinha do Brasil
Responsável	nome: Suzana Brandt Dias e-mail: suzana.brandt@ctim.mar.mil.br telefone (do autor ou responsável): 21 - 2104-7119
Sistemas afetados	**Software**: *Software* de coleta dos dados de votação enviados por cada região eleitoral.
Duração estimada do teste (em minutos)	1440 minutos
Extensão do ataque	☐ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☒ País
Conhecimentos necessários	*Captura de tráfego, criptografia, técnicas de invasão*

2 Reservado ao Tribunal Superior Eleitoral (TSE)

Protocolo	**Data**	
	Resultado ☐ Aprovado ☐ Aprovado com ressalvas ☐ Reprovado	

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

3 Detalhamento do teste

3.1 Resumo do teste

O teste em questão visa explorar possíveis vulnerabilidades dos aplicativos destinados à coleta de informações dos resultados durante a fase de transmissão dos mesmos, mediante interceptação e alteração de informações (man-in-the-middle) e/ou execução remota de programas.

3.2 Fundamentação

Todo equipamento acessado por meio da Internet deverá possuir seus aplicativos com nível de segurança enrijecido (hardening) visando minimizar possíveis explorações. Sendo assim, o sistema de consolidação de dados deve possuir a segurança adequada de forma a identificar e impedir invasões no momento da transferência das informações.

3.3 Precondições para o teste

Software a serem utilizados: Acunetix, Nikto, Backtrack, Samurai, Wireshark

3.4 Escopo – Superfície de Ataque

Os sistemas relacionados com o Teste Público de Segurança não abrange o segmento de transferência supracitado. Uma vez que a Marinha do Brasil possui expertise no trato da tecnologia da informação aplicada a serviços disponibilizados na Internet A Marinha do Brasil se propõe a avaliar e explorar os servidores destinados a captação dos resultados transmitidos via Internet.

3.5 Janela de atuação simulada do atacante

Coleta dos dados transmitidos pela Internet.

3.6 Pontos de intervenção

Firewall e aplicativos do servidor de coleta acessíveis via Internet.

3.7 Passos a serem realizados e material necessário

1. *Varredura dos aplicativos disponibilizados*

2. *Captura de tráfego*
3. *Alteração e injeção de novos dados*
4. *Caso identificadas vulnerabilidades nos aplicativos varridos no item 1, explorar tais vulnerabilidade por meio de shellcode fim execução remota ou acesso remoto ao servidor de coleta dos dados*
5. *Fim.*

3.8 Possíveis resultados e impacto

Durante a fase 1 do item 3.7 não foram apresentados os dados relativos a coleta de informações, desta forma, não há como mensurar a probabilidade do sucesso do ataque pois o mesmo está condicionado à presença de vulnerabilidades no servidor em questão.

.