Índice

Introdução

Este documento descreve o Oracle do estofamento no ataque da criptografia do legado Downgraded (CANICHE) na ferramenta de segurança do email de Cisco (ESA).

Problema

O 3.0 da versão do secure sockets layer (SSL) (RFC-6101) é um Obsoleto e um protocolo inseguro. Quando para a maioria de propósitos práticos, for substituída por seus sucessores - a versão 1.0 do Transport Layer Security (TLS) (RFC-2246), a versão TLS 1.1 (RFC-4346), e a versão TLS 1.2 (RFC-5246) - muitas aplicações TLS permanece para trás? compatível com 3.0 da versão de SSL a fim interoperar com sistemas de legado no interesse de uma experiência lisa do usuário. O aperto de mão do protocolo prevê a negociação de versão autenticada, tão normalmente a versão do protocolo a mais atrasada comum ao cliente e o server é usado. Contudo, mesmo se um cliente e servidor ambos apoia uma versão do TLS, o nível de segurança oferecido pelo 3.0 da versão de SSL é ainda relevante desde que muitos clientes executam uma dança do downgrade do protocolo a fim trabalhar em torno do server? erros laterais da Interoperabilidade.

Os atacantes podem explorar a dança do downgrade e quebrar a segurança criptográfica do 3.0 da versão de SSL. O ataque da CANICHE permite que, por exemplo, roubem? fixe? Cookie HTTP (ou outros tokens do portador tais como índices do encabeçamento da autorização HTTP).

Esta vulnerabilidade foi atribuída as vulnerabilidades e as exposições comuns (CVE) [ID CVE-2014-3566](#).

Solução

Está aqui uma lista de erros relevantes:

- Identificação de bug Cisco [CSCur27131](#) - Ataque da CANICHE do 3.0 da versão de SSL no ESA (CVE-2014-3566)
- Identificação de bug Cisco [CSCur27153](#) - Ataque da CANICHE do 3.0 da versão de SSL no dispositivo do Gerenciamento do Cisco Security (CVE-2014-3566)

- Identificação de bug Cisco CSCur27189 - Ataque da CANICHE do 3.0 da versão de SSL na ferramenta de segurança da Web de Cisco (CVE-2014-3566)

- Identificação de bug Cisco CSCur27340 - Ataque da CANICHE do 3.0 da versão de SSL no dispositivo da criptografia de Cisco Ironport (CVE-2014-3566)

Nos padrões NON-federais do processamento de informação (FIP) modo, o 3.0 da versão de SSL é permitido nas configurações padrão. No FIP-MODE, o 3.0 da versão de SSL é desabilitado à revelia. A fim verificar se o modo FIP é permitido, entre:

```
CLI> fipsconfig

FIPS mode is currently disabled.
```

Quando o modo FIP é desabilitado, verifique se o 3.0 da versão de SSL é permitido nos ajustes do sslconfig. Quando sslv3 é alistado como o método, o 3.0 da versão de SSL está permitido. Mude isto à versão TLS 1 a fim desabilitar o 3.0 da versão de SSL.

```
CLI> sslconfig
sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: <cipher list>
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: <cipher list>
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: <cipher list>
example.com> sslconfig

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> GUI

Enter the GUI HTTPS ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the GUI HTTPS ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
```

```
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> INBOUND

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> OUTBOUND

Enter the outbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the outbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>

example.com> commit
```

```
Please enter some comments describing your changes:
[]> remove SSLv3 from the GUI HTTPS method/Inbound SMTP method/Outbound SMTP method

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Oct 16 07:41:10 2014 GMT
```

Informações Relacionadas

- CVE-2014-3566
- Announcment de Google
- Announcment do OpenSSL
- Suporte Técnico e Documentação - Cisco Systems