Vulnerabilidad CVE-2014-3566 del 3.0 del SSL versión en el ESA

Contenido

Introducción

Este documento describe el Oracle del relleno en el ataque del cifrado de la herencia Downgraded (CANICHE) en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Problema

El 3.0 de la versión de Secure Sockets Layer (SSL) (RFC-6101) es un Obsoleto y un protocolo inseguro. ¿Mientras que para la mayoría de los propósitos prácticos, ha sido substituida por sus sucesores - la versión 1.0 (RFC-2246) de Transport Layer Security (TLS), el TLS versión 1.1 (RFC-4346), y el TLS versión 1.2 (RFC-5246) - muchas implementaciones de TLS permanece al revés? compatible con el 3.0 del SSL versión para interoperar con los sistemas de herencia en interés de una experiencia lisa del usuario. El apretón de manos del protocolo prevé la negociación de la versión autenticada, tan normalmente la última Versión del protocolo común al cliente y se utiliza el servidor. ¿Sin embargo, incluso si un cliente y servidor ambos soporta una versión del TLS, el nivel de seguridad ofrecido por el 3.0 del SSL versión es todavía relevante puesto que muchos clientes implementan una danza del downgrade del protocolo para trabajar alrededor del servidor? bug laterales de la Interoperabilidad.

Los atacantes pueden explotar la danza del downgrade y romper la seguridad criptográfica del 3.0 del SSL versión. ¿El ataque del CANICHE permite que, por ejemplo, roben? ¿asegure? Cookie HTTP (u otros tokens del portador tales como contenido de la encabezado de la autorización HTTP).

Esta vulnerabilidad se ha asignado el Common Vulnerabilities and Exposures (CVE) ID CVE-2014-3566.

Solución

Aquí está una lista de bug relevantes:

- Id. de bug Cisco CSCur27131 - Ataque del CANICHE del 3.0 del SSL versión en el ESA

(CVE-2014-3566)

- Id. de bug Cisco CSCur27153 - Ataque del CANICHE del 3.0 del SSL versión en el dispositivo de la Administración del Cisco Security (CVE-2014-3566)

- Id. de bug Cisco CSCur27189 - Ataque del CANICHE del 3.0 del SSL versión en el dispositivo de seguridad de la red de Cisco (CVE-2014-3566)

- Id. de bug Cisco CSCur27340 - Ataque del CANICHE del 3.0 del SSL versión en el dispositivo del cifrado de Cisco Ironport (CVE-2014-3566)

En los estándares NON-federales del procesamiento de información (FIP) modo, el 3.0 del SSL versión se habilita en las configuraciones predeterminadas. En el FIP-MODE, el 3.0 del SSL versión se inhabilita por abandono. Para marcar si se habilita el modo FIP, ingrese:

```
CLI> fipsconfig

FIPS mode is currently disabled.
```

Cuando se inhabilita el modo FIP, marque si el 3.0 del SSL versión se habilita en las configuraciones del sslconfig. Cuando sslv3 se enumera como el método, se habilita el 3.0 del SSL versión. Cambie esto al TLS versión 1 para inhabilitar el 3.0 del SSL versión.

```
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
```

Información Relacionada

- CVE-2014-3566
- Announcment de Google
- Announcment de Openssl
- Soporte Técnico y Documentación - Cisco Systems