Vulnérabilité CVE-2014-3566 de version 3.0 SSL sur l'ESA

Contenu

Introduction

Ce document décrit Oracle complétant sur l'attaque existante de cryptage Downgraded (CANICHE) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Problème

La version 3.0 (RFC-6101) de Secure Sockets Layer (SSL) est une Désuet(e) et un protocole non sécurisé. Tandis que pour la plupart des fins pratiques, il a été remplacé par ses successeurs - la version 1.0 (RFC-2246) de Transport Layer Security (TLS), la version 1.1 (RFC-4346) de TLS, et la version 1.2 (RFC-5246) de TLS - beaucoup de TLS que les réalisations demeurent vers l'arrière ? compatible avec la version 3.0 SSL afin d'interopérer avec les systèmes existants dans l'intérêt d'une expérience utilisateur sans heurt. La prise de contact de protocole prévoit la négociation authentifiée de version, tellement normalement la dernière version de protocole commune au client et le serveur est utilisé. Cependant, même si un client et un serveur chacun des deux prennent en charge une version de TLS, le niveau de Sécurité offert par la version 3.0 SSL est-il encore approprié puisque beaucoup de clients mettent en application une danse de downgrade de protocole afin de travailler autour du serveur ? bogues latérales d'Interopérabilité.

Les attaquants peuvent exploiter la danse de downgrade et casser la Sécurité cryptographique de la version 3.0 SSL. L'attaque de CANICHE leur permet, par exemple, pour dérober ? sécurisé ? Témoins de HTTP (ou d'autres jetons de support tels que le contenu d'en-tête d'autorisation de HTTP).

Cette vulnérabilité a été assignée l'ID commun CVE-2014-3566 de vulnérabilités et d'expositions (CVE).

Solution

Voici une liste de bogues appropriées :

- ID de bogue Cisco CSCur27131 - Attaque de CANICHE de version 3.0 SSL sur l'ESA (CVE-

2014-3566)

- ID de bogue Cisco CSCur27153 - Attaque de CANICHE de version 3.0 SSL sur l'appliance de Gestion de sécurité Cisco (CVE-2014-3566)
- ID de bogue Cisco CSCur27189 - Attaque de CANICHE de version 3.0 SSL sur l'appliance de sécurité Web de Cisco (CVE-2014-3566)
- ID de bogue Cisco CSCur27340 - Attaque de CANICHE de version 3.0 SSL sur l'appliance de Chiffrement Cisco IronPort (CVE-2014-3566)

En mode de traitement de l'information Non-fédéral des normes (PAP), la version 3.0 SSL est activée dans les valeurs par défaut. En PAP-mode, la version 3.0 SSL est désactivée par défaut. Afin de vérifier si le mode PAP est activé, entrez :

```
CLI> fipsconfig

FIPS mode is currently disabled.
```

Quand le mode PAP est désactivé, vérifiez si la version 3.0 SSL est activée dans les configurations de sslconfig. Quand sslv3 est répertorié comme méthode, la version 3.0 SSL est activée. Changez ceci à la version 1 de TLS afin de désactiver la version 3.0 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
```

Informations connexes

- CVE-2014-3566
- Announcment de Google
- Announcment d'Openssl
- Support et documentation techniques - Cisco Systems