Содержание

Введение

Этот документ описывает атаку Заполнения Oracle на пониженном устаревшем шифровании (POODLE) на Cisco Email Security Appliance (ESA).

Проблема

Версия 3.0 Уровня защищенных сокетов (SSL) (RFC 6101) является устаревшим и незащищенным протоколом. В то время как для наиболее практических целей, это было заменено его преемниками - Версией 1.0 Transport Layer Security (TLS) (RFC 2246), Версия TLS 1.1 (RFC 4346) и Версия TLS 1.2 (RFC 5246) - много реализаций TLS остаются назад? совместимый с Версией SSL 3.0 для взаимодействия с унаследованными системами в интересах плавного пользовательского опыта. Квитирование протокола обеспечивает аутентифицируемое согласование версий, поэтому обычно последняя версия протокола, характерная для клиента и сервера, используется. Однако, даже если клиент и сервер оба поддерживает версию TLS, уровень безопасности, предлагаемый Версией SSL 3.0, все еще релевантен, так как много клиентов внедряют танец перехода на более ранние версии протокола для обхождения сервера? дефекты совместимости стороны.

Атакующие могут использовать танец перехода на более ранние версии и сломать криптографическую безопасность Версии SSL 3.0. Атака POODLE позволяет им, например, красть? безопасный? Cookie HTTP (или другие маркеры несущей, такие как содержание заголовка Авторизации HTTP).

Этой уязвимости назначили Общие Уязвимости и Воздействия (CVE) ID CVE-2014-3566.

Решение

Вот список соответствующих дефектов:

- Идентификатор ошибки Cisco CSCur27131 - Версия SSL 3.0 Атака POODLE на ESA (CVE-2014-3566)
- Идентификатор ошибки Cisco CSCur27153 - Версия SSL 3.0
- Идентификатор ошибки Cisco CSCur27189 - Версия SSL 3.0

- Идентификатор ошибки Cisco CSCur27340 -

В Нефедеральных стандартах обработки информации (FIPS) (FIPS) Режим Версия SSL 3.0 включена в настройках по умолчанию. В Режиме FIPS Версия SSL 3.0 отключена по умолчанию. Чтобы проверить, включен ли режим FIPS, войдите:

```
CLI> fipsconfig

FIPS mode is currently disabled.
```

Когда режим FIPS отключен, проверьте, включена ли Версия SSL 3.0 в sslconfig параметрах настройки. Когда sslv3 перечислен как метод, Версия SSL 3.0 включена. Измените это на Версию TLS 1 для отключения Версии SSL 3.0.

```
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
```

Дополнительные сведения

- CVE-2014-3566
- Google announcment
- Openssl announcment
- Cisco Systems – техническая поддержка и документация