Предотвратите согласования относительно пустых или анонимных шифров на ESA и SMA

ID документа: 117864

Обновлено : 19 февраля 2015

Внесенный Джэем Джиллом и Робертом Шервином, специалистами службы технической поддержки Cisco.

Родственные продукты

- Устройство безопасности электронной почты Cisco

Содержание

Введение

Этот документ описывает, как изменить Cisco Email Security Appliance (ESA) и Устройство менеджмента Cisco Security (SMA) параметры настройки шифра для предотвращения согласований относительно пустых или анонимных шифров. Этот документ применяется к и аппаратным средствам основанные и действительные базирующиеся устройства.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- SMA Cisco

Используемые компоненты

Сведения в этом документе основываются на всех версиях ESA Cisco и SMA Cisco.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Предотвратите согласования относительно пустых или анонимных шифров

В этом разделе описывается предотвратить согласования относительно пустых или анонимных шифров на ESA Cisco, который выполняет AsyncOS для Версий Безопасности электронной почты 9.1 и позже, и также на SMA Cisco.

ESA, который Выполнение AsyncOS для Версии 9.1 Безопасности электронной почты или Позже

Можно модифицировать шифры, которые используются на ESA с **sslconfig** командой. Для предотвращения согласований ESA относительно пустых или анонимных шифров введите **sslconfig** команду в CLI ESA и примените эти параметры настройки:

- Входящий метод Протокола SMTP: **sslv3tlsv1**
- Входящие шифры SMTP: **Средняя - высокая:-SSLv2:-aNULL: СИЛА**
- Исходящий метод SMTP: **sslv3tlsv1**
- Исходящие шифры SMTP: **Средняя - высокая:-SSLv2:-aNULL: СИЛА**

Вот пример конфигурации для входящих шифров:

```
CLI: > 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.
[]> 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]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

> **Примечание:** Установите **GUI**, **ВХОДЯЩИЙ**, и **ИСХОДЯЩИЙ** по мере необходимости для каждого шифра.

С AsyncOS для Версии 8.5 Безопасности электронной почты **sslconfig** команда также доступна через GUI. Для достижения этих параметров настройки от GUI перейдите к **Администрированию системы>, Конфигурации SSL> Редактируют Параметры настройки**:

> **Совет:** Версия 3.0 Защищенных сокетов Лейвера (SSL) (RFC 6101) является устаревшим и незащищенным протоколом. Существует уязвимость в SSLv3 CVE-2014-3566 , известном как *атака Заполнения Oracle на пониженном устаревшем шифровании (POODLE)*, которая отслежена идентификатором ошибки Cisco CSCur27131. Cisco рекомендует отключить SSLv3 при изменении шифров используйте Transport Layer Security (TLS) только и выберите *опцию 3* (v1 TLS). См. идентификатор ошибки Cisco CSCur27131 для завершенных подробных данных.

ESA, который Выполнение AsyncOS для Версии 9.5 Безопасности электронной почты или Позже

С введением AsyncOS для Версии 9.5 Безопасности электронной почты теперь поддерживается v1 2 TLS. Команды, которые описаны в предыдущем разделе все еще, работают; однако, вы будете видеть обновления для v1 2 TLS, включенного в выходные данные.

Вот пример выходных данных от CLI:

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
```

```
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

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/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

Для достижения этих параметров настройки от GUI перейдите к **Администрированию системы> , Конфигурация SSL> Редактирует Параметры настройки...**:

> **Совет:** Для полной информации обратитесь к соответствующему Руководству пользователя ESA для Версии 9.5 или позже.

SMA

sslconfig команда не доступна для SMA Cisco.

> **Примечание:** В это время только v1 TLS поддерживается; v1 2 TLS только поддерживается на ESA.

Необходимо выполнить эти шаги от CLI SMA для изменения шифров SSL:

1. Сохраните файл конфигурации SMA к своему локальному компьютеру.
2. Откройте XML-файл.
3. Ищите *<ssl>* раздел в XML:

```
<ssl>
   <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
   <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
   <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
   <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
   <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
   <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
 </ssl>
```

4. Модифицируйте шифры, как желаемый и сохраните XML:

```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```

5. Загрузите новый файл конфигурации на SMA.

6. **Отправьте** и **передайте** все изменения.

Соответствующие дискуссии сообщества технической поддержки Cisco

Обновлено : 19 февраля 2015
ID документа: 117864