9.5 и более новый AsyncOS для Безопасности электронной почты обновляют с более старыми сертификатами (MD5) связь TLSv1.2 для сбоя

Содержание

[Введение](#)
[Устаревшие сертификаты (MD5) связь причины TLSv1.2 для сбоя на 9.5 AsyncOS для обновлений Безопасности электронной почты и более новый](#)
[Корректирующие изменения](#)
[Корректирующие действия CLI (если к GUI нельзя обратиться),](#)
[Дополнительные сведения](#)
[Соответствующие дискуссии сообщества технической поддержки Cisco](#)

Введение

Этот документ описывает обязательные действия, которые будут применены при обнаружении с проблемой со связью TLS или доступе к веб-интерфейсу, после обновления к AsyncOS для версии 9.5 Безопасности электронной почты или более новый на Устройствах безопасности электронной почты (ESA) Cisco.

Устаревшие сертификаты (MD5) связь причины TLSv1.2 для сбоя на 9.5 AsyncOS для обновлений Безопасности электронной почты и более новый

> **Примечание:** Ниже приводится перечисленный обходной путь для текущих демонстрационных сертификатов, примененных на устройство. Однако ниже шагов может также устройство применяться к любым подписанным сертификатам MD5.

После выполнения обновления к AsyncOS для версии 9.5 Безопасности электронной почты и более новый, любой из устаревших демонстрационных сертификатов IronPort все еще в использовании и просил доставку, получение или LDAP, может столкнуться с ошибками при попытке связаться через TLSv1/TLSv1.2 с некоторыми доменами. Ошибка TLS заставит всех входящих или сеансы исходящего соединения отказывать.

Если сертификаты будут применены к интерфейсу HTTPS, то современные web-браузеры будут не в состоянии обращаться к веб-интерфейсу устройства.

Почтовые Журналы должны выглядеть подобными следующему примеру:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
```

'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Эта ошибка вызвана алгоритмом сигнатуры, применился к более старому сертификату, являющемуся MD5; однако, сертификаты, привязанные к соединяющемуся устройству/браузеру только, поддерживают основанные алгоритмы подписи SHA. Несмотря на то, что более старые демонстрационные сертификаты, который имеет подпись MD5, находятся на устройстве то же время, новый SHA базировал демонстрационный сертификат, который вышеупомянутая ошибка только проявит сама, если подпись MD5 базировалась, сертификат применен к указанным разделам (т.е. получение, доставка, и т.д.)

Ниже пример, который вытягивают от cli устройства, которое имеет обоих более старые сертификаты MD5 в дополнение к новому Демонстрационному Сертификату (Примечание: более новый сертификат (Демонстрация) должен быть более новым алгоритм SHA и иметь более длинную дату окончания действия, чем более старые демонстрационные сертификаты).:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
```

'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')

Корректирующие изменения

1. Перейдите к сети (UI): **Сеть> Сертификаты**
2. Проверьте, что вам в настоящее время устанавливали более старые сертификаты и также имеете новый Демонстрационный сертификат SHA.
3. На основе того, где применены более старые демонстрационные сертификаты, заменяют это новым Демонстрационным сертификатом.

Как правило, эти сертификаты могут быть найдены, будучи примененным в следующих разделах:

- **Сеть> Слушатели> Затем имя слушателя> Сертификат**
- **Почтовые Полицейские> Целевые Средства управления> Редактируют Глобальные параметры> Сертификат**
- **Сеть> IP - интерфейс> Выбирает интерфейс, привязанный к доступу к ГИП> Сертификат HTTPS**
- **Администрирование системы> LDAP> Редактирует Параметры настройки> Сертификат**

4. Как только все сертификаты были заменены, проверяют из командной строки, что связь TLS теперь успешна.

Пример рабочей связи TLS, являющейся договорным использованием TLSv1.2:

```
Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1)
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

Корректирующие действия CLI (если к GUI нельзя

обратиться),

Сертификат, возможно, должен модифицироваться на каждом IP - интерфейсе, которому включили сертификат для сервиса HTTPS. Для изменения сертификата в использовании для интерфейсов выполните следующие команды на CLI:

1. Введите **interfaceconfig**.
2. Выберите **редактируют**.
3. Введите номер интерфейса, который вы хотите отредактировать.
4. Используйте клавишу Return для принятия текущих параметров для каждого представленного вопроса. Когда опция для сертификата для применения будет представлена, выберите Демонстрационный сертификат:
   1.
```
1. Ironport Demo Certificate
2. Demo
Please choose the certificate to apply:
[1]> 2

You may use "Demo", but this will not be secure.
Do you really wish to use the "Demo" certificate? [N]> Y
```
5. Закончите шагать через приглашения параметров настройки, пока не будут завершены все конфигурационные вопросы.
6. Используйте клавишу Return для выхода к основному приглашению CLI.
7. **Usecommit** для сохранения изменений к конфигурации.

Примечание: Не забудьте **передавать** изменения после изменения сертификата в использовании на интерфейсе.

Дополнительные сведения

- Всестороннее руководство по установке для TLS на ESA
- Устройство безопасности электронной почты Cisco - руководства пользователя
- Устройство менеджмента Cisco Security - руководства пользователя
- Cisco Systems – техническая поддержка и документация