SSLv3 и протокол TLSv1 слабая уязвимость режима CBC

Содержание

Введение

Этот документ описывает, как отключить Шифры Режима Cipher Block Chaining (CBC) на Cisco Email Security Appliance (ESA). Проверка защиты / просмотр могла бы сообщить , что ESA имеет V3/Transport Layer Security Уровня защищенных сокетов (SSL) (TLS) Протокол v1 Слабая Уязвимость Режима CBC.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на AsyncOS для Безопасности электронной почты (любой пересмотр), ESA Cisco и действительный ESA.

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.

Общие сведения

- Отраслевой Стандарт по защите данных Платежной карты (DSS PCI) соответствие требует, чтобы были отключены Шифры CBC.
- Проверка защиты / просмотр определила потенциальную уязвимость с протоколами v1 v3/TLS SSL тот Режим CBC использования Шифры.

  Совет: Версия SSL 3.0 (RFC 6101) является устаревшим и незащищенным протоколом. Существует уязвимость в SSLv3 CVE-2014-3566 , известном как атака Заполнения Oracle на пониженном устаревшем шифровании (POODLE), идентификатор ошибки Cisco CSCur27131. В то время как вы изменяете шифры и используете TLS только и выбираете опцию 3 (v1 TLS), рекомендация состоит в том, чтобы отключить v3 SSL. Рассмотрите предоставленный идентификатор ошибки Cisco CSCur27131 для завершенных подробных данных.

V3 SSL и протоколы v1 TLS используются для обеспечения целостности, подлинности и конфиденциальности к другим протоколам, таким как HTTP и Протокол LDAP. Они предоставляют эти сервисы с использованием шифрования для конфиденциальности, x509 сертификаты для подлинности и односторонняя функция шифрования для целостности. Для шифрования данных SSL и TLS могут использовать блочные шифры, которые являются алгоритмами шифрования, которые могут зашифровать только неподвижный блок исходных данных к зашифрованному блоку одинакового размера. Обратите внимание на то, что эти шифры будут всегда получать тот же получающийся блок для того же исходного блока данных. Для достижения различия в выходных данных выходные данные шифрования являются XORed с еще одним блоком одинакового размера, называемого Векторами инициализации (IV). CBC использует один IV для начального блока и результата предыдущего блока для каждого последующего блока для получения различия в выходных данных шифрования блочного шифра.

В v3 SSL и реализации v1 TLS, использование режима CBC выбора было плохо, потому что весь трафик совместно использует один сеанс CBC с отдельным набором начальных IV. Остаток IV является, как упомянуто ранее, результатами шифрования предыдущих блоков. Последующие IV доступны eavesdropper. Это позволяет атакующему с возможностью ввести произвольный трафик в поток простого текста (чтобы быть зашифрованным клиентом) для проверки их предположения простого текста, который предшествует введенному блоку. Если атакующие предполагают, корректно, то выходные данные шифрования являются тем же для двух блоков.

Для низких энтропийных данных возможно предположить блок простого текста с относительно малое число попыток. Например, для данных, которые имеют 1000 возможностей, количество попыток может быть 500.

Требования

Существуют несколька требований, которые должны быть встречены для использования для работы:

1. Соединение SSL/TLS должно использовать один из шифров блочного шифрования, которые используют режим CBC, такой как DES или AES. Каналы, которые используют

поточные шифры, такие как RC4, не подвергаются дефекту. Значительная доля соединений SSL/TLS использует RC4.
2. Уязвимость может только быть использована кем-то, который перехватывает данные на соединении SSL/TLS, и также активно передает новые данные на том соединении. Эксплуатация дефекта заставляет соединение SSL/TLS быть завершенным. Атакующий должен продолжить контролировать и использовать новые соединения, пока достаточно данных не собрано для дешифрования сообщения.
3. Так как соединение завершено каждый раз, клиент SSL/TLS должен быть в состоянии продолжить восстанавливать канал SSL/TLS достаточно долго для сообщения, которое будет дешифровано.
4. Приложение должно повторно передать те же данные на каждом соединении SSL/TLS, которое это создает, и слушатель должен быть в состоянии определить местоположение его в потоке данных. Протоколы как IMAP/SSL, которые имеют неподвижный набор сообщений для регистрации, удовлетворяют это требование. Просмотр общего сетевого трафика не делает.

Угроза

Уязвимость CBC является уязвимостью с v1 TLS. Эта уязвимость была существующей с начала 2004 и была решена в более поздних версиях v1.1 TLS и v1 2 TLS.

До AsyncOS 9.6 для Безопасности электронной почты ESA использует v1.0 TLS и шифры режима CBC. С выпуском AsyncOS 9.6 ESA представляет v1 2 TLS. Однако, шифры режима CBC могут быть отключены, и только шифры RC4 могут использоваться, которые не подвергаются дефекту.

Кроме того, если SSLv2 включают, это может инициировать ошибочный допуск для этой уязвимости. Это очень важно тот SSL v2 быть отключенным.

Решение

Отключите шифры режима CBC для отъезда, только шифры RC4 включили. Заставьте устройство только использовать v1 TLS или v1 2 v1/TLS TLS:

1. Войдите к CLI.
2. Введите команду **sslconfig**.
3. Введите **команду GUI**.
4. Выберите дополнительный номер 3 для "v1 TLS", или, как перечислено в AsyncOS 9.6 "v1 2 v1/TLS TLS".
5. Введите этот шифр:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Введите команду: **ВХОДЯЩИЙ**.
7. Выберите дополнительный номер 3 для "v1 TLS", или, как перечислено в AsyncOS 9.6 "v1 2 v1/TLS TLS".
8. Введите этот шифр:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Введите **команду OUTBOUND**.

10. Выберите дополнительный номер 3 для "v1 TLS", или, как перечислено в AsyncOS 9.6 "v1 2 v1/TLS TLS".
11. Введите этот шифр:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. Нажмите **Enter**, пока вы не возвратитесь к приглашению имени хоста.
13. Введите **передачу** команды.
14. Завершите фиксацию ваших изменений.

ESA теперь настроен, чтобы только поддержать v1 TLS или v1 2 TLSv1/TLS, с шифрами RC4, в то время как это запрещает любые фильтры CBC.

Вот список шифров, используемых при установке RC4:-SSLv2. Обратите внимание на то, что в списке нет никаких шифров режима CBC.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

В то время как это использование представляет очень низкий интерес из-за его сложности и требований для использования, производительность этих шагов является большой гарантией для предотвращения возможного использования, а также передать строгие просмотры безопасности.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация