Отказы подключения SGC: Усиленный и экспортный варианты шифров используют различные дайджесты

Содержание

Введение

Этот документ решает задачу, который происходит в поставщике безопасности файл Schannel.dll, который используется в Microsoft Internet Information Server (IIS) и Microsoft Internet Explorer. Эта проблема представляет, когда вы соединяетесь с узлом, который использует Server Gated Cryptography (SGC), чтобы сделать высокое шифрование, и набор шифров экспорта использует один алгоритм хэширования, в то время как домашний пакет шифрования использует другого. В этой ситуации файл Schannel.dll иногда выбирает неправильный алгоритм, который приводит к сбою подключения. В результате Web - клиенты могут быть не в состоянии соединяться с веб-сайтами, которые используют SGC для строгого шифрования, когда требуется безопасное соединение. Если или Интернет-сервер или Web - клиент выполняют продукты Microsoft, то связь может прерваться.

Microsoft подтверждает, что, когда шифр повышения использует другой дайджест, чем шифр экспорта, может прерваться связь. Для получения дополнительной информации об этой проблеме обратитесь к Сбою мая Подключений SGC от Внутренних Клиентов.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Контент-сервис Cisco (CSS) с модулем Протокола SSL

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Проблема

Со свидетельством повышения SGC на модуле CSS SSL, когда клиентские подключения к узлу через модуль SSL с 56-разрядным браузером, браузер устанавливает подключение SSL в 56 вместо того, чтобы увеличить соединение с 128.

Например, предположите, что первое сообщение приветствия клиента выполняет согласование о шифре rsa-export1024-with-rc4-56-sha. Модуль совпадает на основе заказа в конфигурации (пока шифры не взвешены), поэтому, когда повышение происходит, модуль, вероятно, пытается использовать шифр rsa-with-3des-ede-cbc-sha. Дайджесты этих двух шифров не совпадают, и сбой происходит. Мало того, что дайджесты должны совпасть, BUT, с которым типы шифрования должны совпасть также.

Решение (решения)

На основе прокси-листа клиента в качестве примера решение (решения) этой проблемы объяснено в этом разделе.

В настоящее время у клиента есть эти шифры экспорта:

- ssl-server 4
- адрес ssl-server 4 vip 198.22.10.10
- ssl-server 4 rsakey CSSRsaKey4
- ssl-server 4 rsacert RsaCert4
- шифр ssl-server 4 rsa-with-rc4-128-md5 198.22.10.10 20094
- rsa-with-rc4-128-sha ssl-server 4 шифра 198.22.10.10 20094
- rsa-with-des-cbc-sha ssl-server 4 шифра 198.22.10.10 20094
- шифр ssl-server 4 rsa-with-3des-ede-cbc-sha 198.22.10.10 20094
- шифр ssl-server 4 rsa-export1024-with-des-cbc-sha 198.22.10.10 20094
- rsa-export1024-with-rc4-56-sha ssl-server 4 шифра 198.22.10.10 20094

Решить проблему обсудило в этом документе, необходимо выбрать один шифр экспорта для поддержки (например, rsa-export1024-with-rc4-56-sha). Это обычно - не проблема, потому что, если 56-разрядный браузер передает один из этих шифров, оба передаются. Можно теперь настроить остаток сильных шифров, но необходимо взвесить их таким образом, что шифр (rsa-with-rc4-128-sha) имеет самый высокий вес. Другим сильным

шифрам нужно назначить следующие самые сильные веса, и экспорт зашифровывает самый низкий вес. Вот выборка того, на что эта конфигурация похожа (обратите внимание, что шифр экспорта не имеет никакого веса, поскольку по умолчанию равняется 1):

Примечание: В данном примере у вас есть две опции относительно который набор шифров экспорта использовать. Cisco не может рекомендовать который использовать. Необходимо принять решение на основе бизнес-требований безопасности.

Решение 1

Если вы решаете использовать шифр экспорта (rsa-export1024-with-rc4-56-sha), прокси-лист похож на это:

- rsa-with-rc4-128-sha ssl-server 5 шифра 198.22.124.134 20094 веса 10
- вес rsa-with-rc4-128-md5 198.22.124.134 20094 шифра ssl-server 5 8
- rsa-with-des-cbc-sha ssl-server 5 шифра 198.22.124.134 20094 веса 8
- шифр ssl-server 5 rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 веса 8
- rsa-export1024-with-rc4-56-sha ssl-server 5 шифра 198.22.124.134 20094 веса 1

Решение 2

Если вы решаете поддержать другой шифр экспорта (rsa-export1024-with-des-cbc-sha), ваши веса похожи на это:

- rsa-with-des-cbc-sha ssl-server 5 шифра 198.22.124.134 20094 веса 10
- rsa-with-rc4-128-sha ssl-server 5 шифра 198.22.124.134 20094 веса 8
- вес rsa-with-rc4-128-md5 198.22.124.134 20094 шифра ssl-server 5 8
- шифр ssl-server 5 rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 веса 8
- вес rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 шифра ssl-server 5 1

Дополнительные сведения

- Трафик SSL Настройки через CSS
- Техническая поддержка - Cisco Systems