Содержание

Введение

Этот документ описывает сценарии, в которых веб-страницы Cisco Unified Intelligence Center (CUIC) прекращают загружаться на Internet explorer (IE) после обновлений Базы знаний (KB) установки компонентов доступа к данным корпорации Microsoft.

Статья также предлагает потенциальные обходные пути/решения с точки зрения CUIC.

Предварительные условия

Требования

Cisco рекомендует ознакомиться по этим темам:

- Windows Administration
- Администрирование CUIC и конфигурация

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Cisco унифицированный интеллектуальный центр 10.5 (1)
- Cisco унифицированный интеллектуальный центр 10. x
- Cisco унифицированный интеллектуальный центр 9.1 (x)
- Windows 7 или 8
- Internet Explorer 11

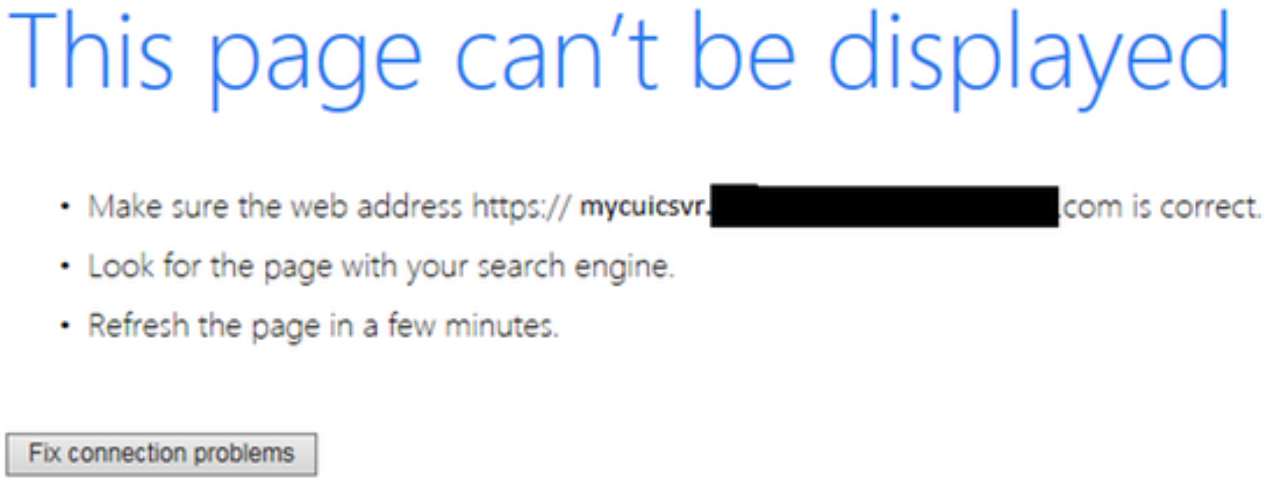
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Сценарий

- Версия 9.1 (1) CUIC или версия 10.5 (1) CUIC

- Internet explorer (IE) 11 на Windows 7 или Windows 8
- Установите KB3161639 на Windows 7/8
- Запустите ссылку CUIC на Internet Explorer - http://<АДРЕС УЗЛА CUIC>*/cuic*

Это вызывает с сообщением об ошибках как показано в образе:



?

Анализ

Microsoft добавила новые Наборы шифров, как показано в образе, как часть свертки обновления июня 2016 KB3161608.

Cipher suite	FIPS mode enabled	Protocols	Exchange	Encryption	Hash
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1

?

Как часть KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** и **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** добавлены к наборам шифров, и заказ приоритета по умолчанию Наборов шифров изменены в Операционной системе Windows.

Из-за этого, если клиентские компьютеры имеют вышеупомянутые обновления, они имеют тенденцию передавать использование **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** с сервером tomcat CUIC (поскольку **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** определен в его config разъёма tomcat CUIC).

Однако связь с помощью шифра **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** не работает. Это вызвано тем, что минимального требования на 1024 бита для ключей Exchange Диффи-Хеллмана (DHE), принужденных Microsoft для решения проблемы атаки затора.

CUIC до версии 11.x имеет Java 6 версий, который только поддерживает ключи на 768 битов. Таким образом это может вызвать сбой квитирования.

Решение

Это не применимо к CUIC 11.0 (1), где решен этот вопрос. Для версий CUIC 9.1 (1) и 10.x версии, это решено открытым файлом COP SSL, доступным здесь

Как часть полицейского openssl, Диффи-Хеллман (DHE) поддержка шифра удалена из разъёма tomcat CUIC путем удаления **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** для предотвращения атаки затора.