Избегите POODLE и POODLE уязвимость BITES при Использовании ASA и AnyConnect

ID документа: 118780

Обновлено : 06 мая 2015

Внесенный Атри Basu, специалист службы технической поддержки Cisco.

Родственные продукты

- Cisco AnyConnect VPN Client
- Устройство адаптивной защиты Cisco (ASA) программное обеспечение
- Secure Socket Layer (SSL)
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility
- Cisco ASA 5500-X Series межсетевые экраны следующего поколения

Содержание

Введение

Этот документ описывает то, что необходимо сделать для предотвращения уязвимости Заполнения Oracle на пониженном устаревшем шифровании (POODLE) при использовании Устройств адаптивной безопасности (ASA) и AnyConnect для подключения Уровня защищенных сокетов (SSL).

Общие сведения

Уязвимость POODLE влияет на определенные реализации протокола Версии 1 Transport Layer Security (TLSv1) и могла позволить не прошедшему поверку подлинности, удаленному атакующему обращаться к уязвимым данным.

Уязвимость происходит из-за неподходящего заполнения блочного шифра, внедренного в TLSv1 при использовании режима Cipher Block Chaining (CBC). Атакующий мог использовать уязвимость для выполнения "оракула, дополняющего" атаку по сторонним каналам на криптографическом сообщении. Успешное использование могло позволить атакующему обращаться к уязвимым данным.

Проблема

ASA позволяет входящие подключения SSL в двух формах:

1. Безклиентый WebVPN
2. AnyConnect Client

Однако ни на одну из реализаций TLS на ASA или клиенте AnyConnect не влияет POODLE. Вместо этого на реализацию SSLv3 влияют так, чтобы любые клиенты (браузер или AnyConnect), которые выполняют согласование о SSLv3, были восприимчивы к этой уязвимости.

> **Внимание. :** POODLE BITES действительно, однако, влияет на TLSv1 на ASA. Для получения дополнительной информации о затрагиваемых продуктах и исправляет, обратитесь к CVE-2014-8730.

Решение

Cisco внедрила эти решения этой проблемы:

1. Все версии AnyConnect, который ранее поддержал (договорной) SSLv3, были осуждены, и версии доступные для скачивания (и v3 1x и v4.0) не выполнят согласование о SSLv3, таким образом, они не будут восприимчивы к проблеме.

2. Параметры протокола ASA по умолчанию были изменены от SSLv3 до TLSv1.0 так, чтобы, пока входящее соединение было от клиента, который поддерживает TLS, об именно это выполнят согласование.

3. ASA может быть вручную настроен для принятия только определенных протоколов SSL с этой командой:

   ssl
   Как упомянуто в решении 1, ни один из в настоящее время поддерживаемых клиентов AnyConnect больше не выполняет согласование о SSLv3, таким образом, клиент будет не в состоянии соединяться с любым ASA, настроенным с любой из этих команд:`ssl server-version sslv3`
   `ssl server-version sslv3-only`
   Однако для развертываний, которые используют v3 0.x и версии AnyConnect v3 1.x,

которые были осуждены (которые являются всеми версиями сборки AnyConnect PRE 3.1.05182), и в котором в частности используется согласование SSLv3, единственное решение состоит в том, чтобы устранить использование SSLv3 или рассмотреть обновление клиентов.

4. Фактическое исправление для POODLE BITES (идентификатор ошибки Cisco CSCus08101) будет интегрировано в последние версии промежуточныйрелиза только. Можно обновить к версии ASA, которая имеет исправление для решения проблемы. Первой доступной версией на Cisco Connection Online (CCO) является Версия 9.3 (2.2).

   Первые неподвижные выпуски ПО ASA для этой уязвимости следующие:
   8.2 Серия: 8.2.5.558.4 Серия: 8.4.7.269.0 Серия: 9.0.4.299.1 Серия: 9.1.69.2 Серия: 9.2.3.39.3 Серия: 9.3.2.2

TLSv1.2

- ASA поддерживает TLSv1.2 с версии программного обеспечения 9.3 (2).
- Клиенты Версии 4.x AnyConnect вся поддержка TLSv1.2.

Это означает:

- При использовании Безклиентый WebVPN, то любой ASA, который выполняет эту версию ПО или выше может выполнить согласование о TLSv1.2.

- При использовании клиента AnyConnect для использования TLSv1.2, необходимо будет обновить клиентам Версии 4.x.

Дополнительные сведения

- CVE-2014-8730
- Идентификатор ошибки Cisco CSCug51375
- Идентификатор ошибки Cisco CSCur42776
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 06 мая 2015
ID документа: 118780