Сервер Cisco Collaboration 5.0: Устранение уязвимостей системы безопасности, вызванных методами HTTP TRACE/TRACK

Содержание

Введение

Этот документ обращается к шагам для обхождения уязвимости безопасности, вызванной методами ТРАССИРОВКИ/ДОРОЖКИ HTTP для продуктов, которые используют Microsoft Internet Information Services (IIS) в качестве веб-сервера. Cisco Collaboration Server 5.0 IIS 5.0 использования как веб-сервер и восприимчив к этой уязвимости. Решение состоит в том, чтобы использовать утилиту URLScan Microsoft для отключения методов ТРАССИРОВКИ/ДОРОЖКИ HTTP.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Microsoft Windows 2000 Server
- Сервер Cisco Collaboration 5.0
- Microsoft IIS 5.0
- Утилита Microsoft URLScan

Используемые компоненты

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

- Microsoft Windows 2000
- Версии Cisco Collaboration Server 5.0
- Microsoft IIS 5 (при использовании Windows 2000)
- Microsoft URLScan 2.5

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

HTTP веб-сервера ОТСЛЕЖИВАЕТ/ОТСЛЕЖИВАЕТ Уязвимость Отслеживания перекрестного Узла Поддержки Метода

Веб-сервер был обнаружен, который поддерживает метод ТРАССИРОВКИ HTTP. Этот метод позволяет отлаживать и анализ Трассировки связи для соединений от клиента к веб-серверу. На Спецификацию HTTP, когда этот метод используется, веб-сервер реагирует на информацию, передаваемую ему клиентом, немодифицированным и нефильтруемым. Веб-сервер Microsoft IIS использует ДОРОЖКУ псевдонима для этого метода и является функционально тем же.

Была обнаружена уязвимость, отнесенная к этому методу. Злонамеренный, активный компонент в веб-странице может отправить запросы ТРАССИРОВКИ к веб-серверу, который поддерживает этот метод ТРАССИРОВКИ. Обычно, безопасность браузера запрещает доступ к веб-сайтам за пределами домена существующего узла. Несмотря на то, что маловероятный и трудный достигнуть, возможно, в присутствии других уязвимостей браузера, для активного содержимого HTML выполнить внешние запросы к произвольным веб-серверам вне веб-сервера хостинга. Поскольку выбранный веб-сервер тогда реагирует на нефильтруемый запрос клиента, ответ также включает основанный на cookie или находящийся на web (если вошедшийся в систему) учетные данные для аутентификации, которые браузер автоматически передал к указанному web - приложению на указанном веб-сервере. Значение возможности ТРАССИРОВКИ в этой уязвимости состоит в том, что активный компонент на странице, которую посещает пользователь жертвы, не имеет никакого прямого доступа к этой информации для аутентификации, но получает его после того, как целевой веб-сервер повторяет его назад как ответ ТРАССИРОВКИ. Поскольку эта уязвимость существует как поддержка метода, требуемого спецификацией HTTP - протокола, наиболее распространенные веб-серверы уязвимы.

Microsoft IIS: Microsoft освободила **URLScan** (http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp), который может использоваться для экранирования всех входящих запросов на основе специализированного rulesets. URLScan может использоваться, чтобы санировать или отключить запросы ТРАССИРОВКИ от клиентов. Обратите внимание на то, что IIS искажает ДОРОЖКУ для ОТСЛЕЖИВАНИЯ. Поэтому, если URLScan используется для специфического блокирования метода ТРАССИРОВКИ, метод ДОРОЖКИ должен также быть добавлен к фильтру. URLScan использует urlscan.ini файл конфигурации, обычно в **\System32\InetSrv\URLScan** каталоге.

В этом существует два раздела: `AllowVerbs` и `DenyVerbs`. Если переменная `UseAllowVerbs` установлена в **1,** прежний используется; иначе (если установлено в 0), `DenyVerbs`

используется. Безусловно, или может использоваться, в зависимости от того, хотите ли вы Default-Deny-Explicit-Allow или Default-Allow-Explicit-Deny политику. Для запрещения ТРАССИРОВКИ и методов ДОРОЖКИ через URLScan, сначала удалите ДОРОЖКУ, ОТСЛЕДИТЕ методы от AllowVerbs, разделяют и добавляют их к разделу DenyVerbs. С этим URLScan будет запрещать всю ТРАССИРОВКУ и ОТСЛЕЖИВАТЬ методы и генерировать ошибочную страницу для всех запросов с помощью того метода. Для включения изменений перезапустите Сервис веб-публикации от **Сервисов>** элемент **Панели управления**.

Установите и настройте версию программы 2.5 URLScan для отключения метода ТРАССИРОВКИ/ДОРОЖКИ HTTP

Выполните следующие действия:

1. Установите URLScan 2.5 в Cisco Collaboration Server. Для загрузки URLScan 2.5 обратитесь к этому Веб-узлу Microsoft:http://microsoft.com/downloads/details.aspx?FamilyId=23D18937-DD7E-4613-9928-7F94EF1C902A&displaylang=en
2. Отредактируйте urlscan.ini подарок файла свойств в **<дисковод установки сервера Windows 2000>:\WINNT\system32\inetsrv\urlscan**.
3. Измените свойство `AllowDotinPath` от 0 до 1. По умолчанию URLScan не позволяет точки в URL, и Cisco Collaboration Server требует, чтобы это свойство было установлено в 1 (агенты не будут в состоянии войти, если это свойство будет установлено в 0).
4. Добавьте ТРАССИРОВКУ и ОТСЛЕДИТЕ методы под разделом `DenyVerbs` и измените свойство `AllowVerbs` от 1 до 0.
5. Информационные сервисы интернета (IIS) перезапуска / сервисы Всемирной паутины от **Сервисов>** элемент **Панели управления** на Cisco Collaboration Server.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация