Nmap Показывает, что CCM Восприимчив к Атаке SWEET32

Содержание

Введение

Этот документ описывает проблему, где Nmap показывает, что Cisco Call Manager (CCM) восприимчив к Атаке SWEET32.

Проблема

При выполнении Nmap 4.70 + вы видите предупреждающие сообщения о Стандарт тройного шифрования данных (3DES) и IDEA, которые показывают, что это уязвимо для SWEET32.

```
nmap -sV --script ssl-enum-ciphers -p 443 <ip_of_ccm>
```

Неделя 64-разрядное шифрование была найдена восприимчивой к атаке, известной как Sweet32. Новые версии Nmap будут включать проверку, чтобы видеть, включены ли какие-либо шифры, которые восприимчивы. Из-за этого, выполняя просмотр Nmap на CCM отображает это предупреждение:

```
64-bit block cipher 3DES vulnerable to SWEET32 attack

64-bit block cipher IDEA vulnerable to SWEET32 attack
```

Решение

Эта проблема непосредственно не отнесена к CloudCenter, но серверу Tomcat это использование cloudcenter. Нужно обратить внимание, что просмотр Nmap не сообщает, что Виртуальная машина (VM) уязвима для атаки, это просто сообщает, что использует шифр, который уязвим. Существуют другие переменные, которые требуются, чтобы существовать для этой атаки для следования, тот Nmap не тестирует на.

Базовый билет; БАЗОВЫЕ 15086 были созданы относительно этого. Решение все еще находится под процессом, и версия OpenSSL 1.1.0 + обновлена, который в свою очередь исправит дефект.

Разработка сообщила, что сообщение об ошибках может быть безопасно проигнорировано, однако, в случае необходимости существует обходной путь.

Secure Shell (SSH) в CCM.

Открытый**/usr/local/tomcat/conf/server.xml**.

Прокрутите вниз, пока вы не находите раздел, который запускается с **<Порт разъёма = "10443"**.

```
    <Connector port="10443" maxHttpHeaderSize="8192"
               maxThreads="150"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               SSLEnabled="true"
               SSLCertificateFile="${catalina.base}/conf/ssl/example.com.crt"
               SSLCertificateKeyFile="${catalina.base}/conf/ssl/example.com.key"
               SSLCACertificateFile="${catalina.base}/conf/ssl/gd_bundle.crt"
               SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
               SSLCipherSuite="ALL:!aNULL:!EDH:!ADH:!eNULL:!LOW:!EXP:!RC4:+HIGH:+MEDIUM"
               compression="on" compressionMinSize="2048"
               compressableMimeType="text/html,text/xml,text/plain,application/javascript,application/json,text/javascript,text/css,application/css,image/x-icon,image
jpeg,image/png,image/svg+xml,application/x-shockwave-flash,application/x-java-jnlp-file,application/zip,application/x-font-ttf,application/x-font-opentype,application
x-font-woff,application/vnd.ms-fontobject" />

     <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="100"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               SSLEnabled="true"
               SSLCertificateFile="${catalina.base}/conf/ssl/mgmtserver.crt"
               SSLCertificateKeyFile="${catalina.base}/conf/ssl/mgmtserver.key"
               SSLCACertificateFile="${catalina.base}/conf/ssl/ca.crt"
               SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
               SSLCipherSuite="ALL:!aNULL:!EDH:!ADH:!eNULL:!LOW:!EXP:!RC4:+HIGH:+MEDIUM"
               SSLVerifyClient="require" />
```

Линия, которая запускается с SSLCipherSuite =, перечисляет шифры, которые позволены и не позволены.

В конце каждой из тех линий добавьте **:! 3DES:! IDEA**

После начала Tomcat 3DES и IDEA больше не будут использоваться и таким образом, просмотр Nmap больше не будет сообщать ни о каких предупреждениях.

> **Примечание:** Этот обходной путь не был протестирован на совместимость, и некоторые пользователи больше не могли бы быть в состоянии соединиться с Интерфейсом пользователя (UI) CCM. Пользователи с Windows XP и те, которые выполняют IE v8, не могли бы быть в состоянии соединиться больше. Однако это не было протестировано.