Nmap zeigt, dass CCM anfällig für SWEET32-Angriffe ist

Inhalt

Einführung

In diesem Dokument wird ein Problem beschrieben, bei dem Nmap anzeigt, dass der Cisco Call Manager (CCM) anfällig für SWEET32-Angriffe ist.

Problem

Wenn Sie Nmap 4.70+ ausführen, sehen Sie Warnmeldungen über Triple Data Encryption Standard (3DES) und IDEA, die zeigen, dass es anfällig für SWEET32 ist.

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

64-Bit-Verschlüsselungen in Woche wurden als anfällig für einen Angriff mit der Bezeichnung Sweet32 identifiziert. Neue Versionen von Nmap enthalten eine Überprüfung, ob anfällige Chiffren aktiviert sind. Daher wird beim Ausführen der Nmap-Prüfung auf dem CCM folgende Warnung angezeigt:

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

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

Lösung

Dieses Problem steht nicht in direktem Zusammenhang mit CloudCenter, sondern mit dem Tomcat-Server, den CloudCenter verwendet. Es ist zu beachten, dass der Nmap-Scan nicht angibt, dass das virtuelle System (VM) für den Angriff anfällig ist, sondern lediglich angibt, dass es einen angreifbaren Code verwendet. Es gibt weitere Variablen, die vorhanden sein müssen, damit dieser Angriff erfolgreich verläuft, auf die Nmap nicht testet.

ein Kernticket; Hierfür wurde CORE-15086 erstellt. Die Lösung ist noch in Bearbeitung und die Version von OpenSSL 1.1.0+ wird aktualisiert, was wiederum den Fehler korrigieren wird.

Engineering hat erklärt, dass die Fehlermeldung sicher ignoriert werden kann, aber es gibt eine Lösung, wenn nötig.

Secure Shell (SSH) in den CCM.

Öffnen Sie **/usr/local/tomcat/conf/server.xml**.

Blättern Sie nach unten, bis Sie den Abschnitt finden, der mit **<Connector port="10443"** beginnt.

```
    <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" />
```

Die Zeile, die mit SSLCipherSuite= beginnt, listet die zulässigen und nicht zulässigen Verschlüsselungen auf.

Am Ende jeder dieser Posten fügen Sie Folgendes hinzu: **!3DES:!IDEA**

Nach dem Start Tomcat, 3DES und IDEA wird nicht mehr verwendet und so die Nmap? Die Prüfung meldet keine Warnungen mehr.

> **Hinweis**: Diese Problemumgehung wurde nicht auf Kompatibilität getestet, und einige Benutzer können möglicherweise nicht mehr auf die CCM-Benutzeroberfläche zugreifen. Benutzer mit Windows XP und Benutzer, die IE v8 ausführen, können möglicherweise keine Verbindung mehr herstellen. Es wurde jedoch nicht getestet.