Nmap muestra que CCM es susceptible al ataque SWEET32

Contenido

Introducción

Este documento describe un problema donde Nmap muestra que el Cisco Call Manager (CCM) es susceptible al ataque SWEET32.

Problema

Cuando usted ejecuta Nmap 4.70+, usted ven los mensajes de advertencia sobre el Estándar de triple cifrado de datos (3DES) y la IDEA que muestran que son vulnerables a SWEET32.

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

Los cifrados 64-bit de la semana se han encontrado susceptibles a un ataque conocido como Sweet32. Las nuevas versiones de Nmap incluirán un control para considerar si se habilitan algunas cifras que sean susceptibles. Debido a esto, funcionar con la exploración de Nmap en CCM visualiza esta advertencia:

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

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

Solución

Este problema no se relaciona directamente con CloudCenter, sino el servidor de Tomcat que las aplicaciones del cloudcenter. Debe ser observado que el Nmap que la exploración no estado que la máquina virtual (VM) es vulnerable al ataque, él estado simplemente que utiliza una cifra que sea vulnerable. Hay otras variables que se requieren existir para que este ataque tenga éxito que Nmap no prueba para.

Un boleto de la base; CORE-15086 se ha creado en lo que respecta a esto. La solución todavía está bajo proceso y la versión del OpenSSL 1.1.0+ es actualizada que a su vez parcheará el defecto.

La ingeniería ha expuesto que el mensaje de error se puede ignorar con seguridad, sin embargo, hay una solución alternativa si es necesario.

Secure Shell (SSH) en CCM.

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

Navegue hacia abajo hasta que usted encuentre la sección que comienza con el **<Connector el port="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" />
```

La línea que comienza con SSLCipherSuite= enumera las cifras se permiten y no se permiten que.

¡En el final de cada uno de esas líneas agregue:**! 3DES:!IDEA**

¿Después de que usted comience Tomcat, el 3DES y la IDEA serán utilizados no más y tan el Nmap? la exploración señalará no más cualquier advertencia.

> Nota: Esta solución alternativa no se ha probado para la compatibilidad y algunos usuarios pudieron no más poder conectar con CCM la interfaz de usuario (UI). Los usuarios con Windows XP y los que ejecutan IE v8 no pudieron poder conectar más. Sin embargo, no se ha probado.