Nmap indica che CCM è suscettibile a un attacco SWEET32

Sommario

Introduzione

Questo documento descrive un problema in cui Nmap mostra che Cisco Call Manager (CCM) è suscettibile di attacchi SWEET32.

Problema

Quando si esegue Nmap 4.70+, vengono visualizzati messaggi di avviso relativi a Triple Data Encryption Standard (3DES) e IDEA che indicano che è vulnerabile a SWEET32.

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

La crittografia a 64 bit della settimana è stata rilevata suscettibile a un attacco noto come Sweet32. Le nuove versioni di Nmap includeranno un controllo per verificare se sono abilitate eventuali cifrature sensibili. Per questo motivo, l'esecuzione della scansione Nmap su CCM visualizza questo avviso:

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

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

Soluzione

Questo problema non è direttamente correlato a CloudCenter, ma al server Tomcat utilizzato da cloudcenter. Va notato che la scansione Nmap non indica che la macchina virtuale (VM) è vulnerabile all'attacco, ma semplicemente che utilizza una cifratura vulnerabile. Per la riuscita di questo attacco sono necessarie altre variabili che Nmap non è in grado di testare.

Biglietto di base; Per questo motivo è stato creato il CORE-15086. La soluzione è ancora in fase di elaborazione e la versione di OpenSSL 1.1.0+ viene aggiornata per risolvere il problema.

Il reparto di progettazione ha dichiarato che il messaggio di errore può essere ignorato. Se necessario, è disponibile una soluzione alternativa.

Secure Shell (SSH) nel CCM.

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

Scorrere verso il basso fino a individuare la sezione che inizia con **<Connector 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 riga che inizia con SSLCipherSuite= elenca le cifrature consentite e non consentite.

Alla fine di ognuna di queste righe aggiungere: **!3DES:!IDEA**

Dopo l'avvio di Tomcat, 3DES e IDEA non verranno più utilizzati, quindi Nmap? l'analisi non segnalerà più alcun avviso.

> **Nota:** Questa soluzione non è stata testata per verificarne la compatibilità e alcuni utenti potrebbero non essere più in grado di connettersi all'interfaccia utente di CCM. Gli utenti di Windows XP e di Internet Explorer v8 potrebbero non essere più in grado di connettersi. Tuttavia, non è stato testato.