Nmap prouve que CCM est susceptible de l'attaque SWEET32

Contenu

Introduction

Ce document décrit une question où Nmap prouve que le Cisco Call manager (CCM) est susceptible de l'attaque SWEET32.

Problème

Quand vous exécutez Nmap 4.70+, vous voyez les messages d'avertissement au sujet du Norme 3DES (Triple Data Encryption Standard) et l'IDÉE qui prouvent qu'ils sont vulnérables à SWEET32.

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

Les cryptages 64-bit de semaine ont été susceptibles trouvé d'une attaque connue sous le nom de Sweet32. Les nouvelles versions de Nmap incluront un contrôle pour voir si on active des chiffrements qui sont susceptibles. Pour cette raison, exécuter le balayage de Nmap sur le CCM affiche cet avertissement :

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

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

Solution

Cette question n'est pas directement liée à CloudCenter, mais au serveur de Tomcat que des utilisations de cloudcenter. Il convient noter que le balayage de Nmap ne déclare pas que le virtual machine (VM) est vulnérable à l'attaque, il déclare simplement qu'il utilise un chiffrement qui est vulnérable. Il y a d'autres variables qui sont exigées pour être en place pour que cette attaque réussisse que Nmap ne détermine pas.

Un principal ticket ; CORE-15086 a été créé quant à ceci. La solution est toujours sous le processus et la version d'OpenSSL 1.1.0+ est mise à jour qui à leur tour corrigera l'imperfection.

L'ingénierie a déclaré que le message d'erreur peut être sans risque ignoré, cependant, il y a un contournement si nécessaire.

Protocole Secure Shell (SSH) dans le CCM.

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

Faites descendre l'écran jusqu'à ce que vous trouviez la section qui commence par le **<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 ligne qui commence par SSLCipherSuite= répertorie les chiffrements qui sont permis et pas permis.

Àla fin de chacune de ces lignes ajoutez : **! 3DES:!IDEA**

Après que vous commenciez Tomcat, 3DES et IDÉE ne seront-ils plus utilisés et ainsi le Nmap ? le balayage ne signalera plus aucun avertissement.

> Remarque: Ce contournement n'a pas été testé pour la compatibilité et quelques utilisateurs pourraient plus ne pouvoir se connecter à l'interface utilisateur CCM (UI). Les utilisateurs avec Windows XP et ceux qui exécutent IE v8 ne pourraient pas pouvoir se connecter plus. Cependant, il n'a pas été testé.