Nmap toont aan dat CCM vatbaar is voor SWEET32-aanval

Inhoud

Inleiding

Dit document beschrijft een probleem waar Nmap aangeeft dat Cisco Call Manager (CCM) vatbaar is voor SWET32-aanvallen.

Probleem

Wanneer u Nmap 4.70+ gebruikt, ziet u waarschuwingsberichten over Triple Data Encryption Standard (3DES) en IDEA die aantonen dat dit kwetsbaar is voor SWEET32.

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

Week 64-bits encrypties zijn vatbaar bevonden voor een aanval die bekend staat als Sweet32. Nieuwe versies van Nmap zullen een controle omvatten om te zien of er cifen zijn ingeschakeld die gevoelig zijn. Daarom wordt in het uitvoeren van de Nmap-scan op het CCM deze waarschuwing weergegeven:

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

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

Oplossing

Dit probleem is niet direct gerelateerd aan CloudCenter, maar de Tomcat-server die cloudcenter gebruikt. Er zij op gewezen dat de Nmap-scan niet aangeeft dat de virtuele machine (VM) kwetsbaar is voor de aanval, maar alleen aangeeft dat hij een kwetsbaar algoritme gebruikt. Er zijn andere variabelen die vereist zijn om deze aanval te laten slagen waarvoor Nmap niet test.

een kernticket; In dit verband is CORE-15086 opgericht. De oplossing is nog steeds in proces en de versie van OpenSSL 1.1.0+ wordt bijgewerkt, waardoor de fout wordt gedempt.

Engineering heeft verklaard dat de foutmelding veilig kan worden genegeerd, maar dat er indien nodig een tijdelijke oplossing is.

Secure Shell (SSH) in het CCM.

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

Scrolt neer tot u het gedeelte vindt dat begint met **<Connector poort="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" />
```

De lijn die met SSLCipherSuite begint maakt een lijst van de ciphers die zijn toegestaan en niet toegestaan.

Aan het eind van elk van deze regels voegt u toe: **!3DES:!IDEA**

Nadat je Tomcat start, zullen 3DES en IDEA niet meer gebruikt worden, dus de Nmap? scan zal geen waarschuwingen meer melden .

> Opmerking: Deze workround is niet getest op compatibiliteit en sommige gebruikers kunnen niet langer verbinding maken met de CCM User Interface (UI). Gebruikers met Windows XP en gebruikers die IE v8 gebruiken kunnen mogelijk geen verbinding meer maken. Het is echter niet getest.