Nmap mostra que o CCM é susceptível ao ataque SWEET32

Índice

Introdução

Este documento descreve uma edição onde Nmap mostre que o Cisco Call Manager (CCM) é susceptível ao ataque SWEET32.

Problema

Quando você executa Nmap 4.70+, você veem os mensagens de advertência sobre o Triple Data Encryption Standard (3DES) e o IDEA que mostram que são vulneráveis a SWEET32.

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

As criptografias 64-bit da semana foram encontradas susceptíveis a um ataque conhecido como Sweet32. As novas versões de Nmap incluirão uma verificação para considerar se alguma cifra é permitida que for susceptível. Devido a isto, executar a varredura de Nmap no CCM indica este aviso:

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

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

Solução

Esta edição não é relacionada diretamente a CloudCenter, mas ao server de Tomcat que usos do cloudcenter. Deve-se notar que a varredura de Nmap não indica que a máquina virtual (VM) é vulnerável ao ataque, ele indica meramente que usa uma cifra que seja vulnerável. Há outras variáveis que são exigidas ser no lugar para que este ataque suceda que Nmap não testa para.

Um bilhete do núcleo; CORE-15086 foi criado a propósito deste. A solução é ainda abaixo processo e a versão do OpenSSL 1.1.0+ é atualizada que por sua vez remendará a falha.

A engenharia indicou que o Mensagem de Erro pode com segurança ser ignorado, contudo, há uma ação alternativa se necessário.

Shell Seguro (ssh) no CCM.

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

Enrole para baixo até que você encontre a seção que começa com **<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" />
```

A linha que começa com SSLCipherSuite= alista as cifras que são permitidas e não permitidas.

No fim de cada um daquelas linhas adicionar:**! 3DES:!IDEA**

Depois que você começa Tomcat, 3DES e IDEA estará usado já não e assim o Nmap? a varredura já não relatará todos os avisos.

> Nota: Esta ação alternativa não foi testada para a compatibilidade e alguns usuários puderam já não poder conectar à interface do utilizador CCM (UI). Os usuários com Windows XP e aqueles que executam IE v8 não puderam poder conectar anymore. Contudo, não foi testado.