Nmap显示CCM易受SWEET32攻击

目录

简介

本文档介绍Nmap显示Cisco Call Manager(CCM)易受SWEET32攻击的问题。

问题

运行Nmap 4.70+时，您会看到有关三重数据加密标准(3DES)和IDEA的警告消息，这些消息显示它易受SWEET32攻击。

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

第64周的加密易受名为Sweet32的攻击。新版Nmap将包括检查是否启用了易受攻击的密码。因此，在CCM上运行Nmap扫描会显示以下警告：

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

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

解决方案

此问题与CloudCenter不直接相关，而是与CloudCenter使用的Tomcat服务器有关。应注意，Nmap扫描不表示虚拟机(VM)易受攻击，而只是表示它使用易受攻击的密码。为了使此攻击成功，Nmap不测试，还需要设置其他变量。

核心票；CORE-15086已创建。该解决方案仍在处理中，OpenSSL 1.1.0+版本将更新，这进而会修补该缺陷。

工程部门已声明可以安全地忽略错误消息，但是，如有需要，可以采取解决方法。

安全外壳(SSH)连接到CCM。

打开**/usr/local/tomcat/conf/server.xml**。

向下滚动，直到找到以<Connector port="10443"**开头的部分**。

```
    <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" />
```

以SSLCipherSuite=开头的行列出了允许和不允许的密码。

在每行末尾添加：**!3DES:!IDEA**

启动Tomcat后，3DES和IDEA将不再使用，因此Nmap?扫描将不再报告任何警告。

> **注意**：此解决方法尚未测试兼容性，某些用户可能无法再连接到CCM用户界面(UI)。 使用Windows XP和运行IE v8的用户可能无法再连接。但是，它尚未经过测试。