Nmap显示CCM是易受SWEET32攻击

目录

简介

本文描述Nmap显示的问题Cisco Call Manager (CCM)是易受SWEET32攻击。

问题

当您运行Nmap 4.70+时，您看到显示关于三重数据加密标准(3DES)的警告消息和IDEA是易受攻击对SWEET32。

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

找到了周64位加密易受影响作为Sweet32被称作的攻击。Nmap新版本将包括检查发现是易受的任何密码器是否启用。因此，运行在CCM的Nmap扫描显示此警告：

```
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，然而Tomcat服务器没有直接地涉及cloudcenter用途。值得注意的是，Nmap扫描不阐明，虚拟机易受到攻击，它仅仅阐明，使用易受攻击的一密码器。有要求是到位为了此攻击能成功的其他变量Nmap不测试对于。

核心票;CORE-15086创建关于此。解决方案仍然是下进程，并且反之将修补缺点的版本Openssl 1.1.0+更新。

工程阐明，然而，错误消息可以安全忽略若需要有应急方案。

安全壳SSH到CCM里。

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

请移下来，直到您查找从**<Connector port="10443"**开始的部分。

```
    <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" />
```

从SSLCipherSuite=启动的线路列出允许和没有允许的密码器。

在那些线路中的每一条结束时请添加：**!3DES:!IDEA**

在您开始Tomcat后，不再将使用3DES是否和IDEA和如此Nmap ？扫描不再将报告所有警告。

> **注意**：此应急方案未为兼容性测试，并且一些用户也许不再能连接到CCM用户界面(UI)。运行IE V-8有Windows XP的用户和那些也许不能再连接。然而，它未测试。