Nmapは、CCMがSWEET32攻撃を受けやすい性質を示す

内容

概要

このドキュメントでは、NmapがCisco Call Manager(CCM)がSWEET32攻撃の影響を受けやすいことを示す問題について説明します。

問題

Nmap 4.70+を実行すると、トリプルData Encryption Standard(3DES)およびIDEAに関する警告メッセージが表示され、これがSWEET32に対して脆弱であることが示されます。

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

Sweet32と呼ばれる攻撃の影響を受けやすい64ビット暗号化が週64回発見されました。新しいバージョンのNmapには、影響を受けやすい暗号が有効になっているかどうかを確認するチェックが含まれます。このため、CCMでNmapスキャンを実行すると、次の警告が表示されます。

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

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

解決方法

この問題は、CloudCenterに直接関連するものではなく、cloudcenterが使用するTomcatサーバに関連するものです。Nmapスキャンは、仮想マシン(VM)が攻撃に対して脆弱であることを示すものではなく、単に脆弱な暗号を使用していることを示すものであることに注意してください。この攻撃を成功させるために、Nmapがテストしていない他の変数も設定しておく必要があります。

コアチケットこれに関してCORE-15086が作成されました。ソリューションはまだ処理中であり、OpenSSL 1.1.0+のバージョンが更新され、欠陥にパッチが適用されます。

エンジニアリングでは、このエラーメッセージは無視しても問題ありませんが、必要に応じて回避策があります。

CCMへのセキュアシェル(SSH)。

/usr/local/tomcat/conf/server.xml を開く.

<Connector port="10443"で始まるセクションが見つかるまで下にスクロールします。

```
    <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" />
```

SSLCipherSuite=で始まる行には、許可されている暗号と許可されていない暗号がリストされます。

それぞれの行の終わりに次を追加します：!3DES:!IDEA

Tomcatを起動すると、3DESとIDEAは使用されなくなるため、Nmapは使用されますか。スキャンは警告を報告しません。

> **注**：この回避策は互換性がテストされておらず、一部のユーザがCCMユーザインターフェイス(UI)に接続できない可能性があります。 Windows XPおよびIE v8を実行するユーザは、接続できなくなる可能性があります。ただし、まだテストされていません。