Nmap顯示CCM易受SWEET32攻擊

目錄

簡介

本文檔描述了Nmap顯示Cisco Call Manager(CCM)易受SWEET32攻擊的問題。

問題

運行Nmap 4.70+時，您會看到有關三重資料加密標準(3DES)和IDEA的警告消息，表明它易受SWEET32攻擊。

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

第64週發現，64位加密容易遭受名為Sweet32的攻擊。新版Nmap將包括一個檢查以確認是否已啟用易受攻擊的密碼。因此，在CCM上運行Nmap掃描將顯示以下警告：

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

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

解決方案

此問題與CloudCenter沒有直接關係，而是與cloudcenter使用的Tomcat伺服器有關。應注意，Nmap掃描並未指出虛擬機器(VM)易受攻擊，只是指出它使用易受攻擊的密碼。Nmap未測試的其他變數必須到位，該攻擊才能成功。

一張核心票；CORE-15086已建立與此相關。該解決方案仍在處理中，OpenSSL 1.1.0+的版本也進行了更新，這反過來將修補該漏洞。

工程界已經宣告可以安全地忽略該錯誤資訊，但是如果有需要，可以採取一種解決方法。

安全外殼(SSH)進入CCM。

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

向下滾動，直到找到以<Connector port="**10443"開頭的部分**。

```
    <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=開頭的行列出允許和不允許的密碼。

每行末尾都新增： **!3DES:!IDEA**

啟動Tomcat後，將不再使用3DES和IDEA，因此不再使用Nmap?掃描將不再報告任何警告。

> **附註**：此解決方法尚未經過相容性測試，某些使用者可能無法再連線到CCM使用者介面(UI)。使用Windows XP和運行IE v8的使用者可能無法再連線。然而，它尚未經過測試。