Nmap Shows that CCM is Susceptible to SWEET32 Attack

Contents

[Introduction](#)
[Problem](#)
[Solution](#)

Introduction

This document describes an issue where Nmap shows that the Cisco Call Manager (CCM) is susceptible to SWEET32 Attack.

Problem

When you run Nmap 4.70+, you see warning messages about Triple Data Encryption Standard (3DES) and IDEA that show that it is vulnerable to SWEET32.

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

Week 64-bit encryptions have been found susceptible to an attack known as Sweet32. New versions of Nmap will include a check to see if any ciphers are enabled that are susceptible. Because of this, running the Nmap scan on the CCM displays this warning:

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

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

Solution

This issue is not directly related to CloudCenter, but the Tomcat server that cloudcenter uses. It should be noted that the Nmap scan does not state that the Virtual Machine (VM) is vulnerable to the attack, it merely states that it uses a cipher that is vulnerable. There are other variables that are required to be in place in order for this attack to succeed that Nmap does not test for.

A core ticket; CORE-15086 has been created with regards to this. The solution is still under process and version of OpenSSL 1.1.0+ is updated which in turn will patch the flaw.

Engineering has stated that the error message can be safely ignored, however, there is a workaround if needed.

Secure Shell (SSH) into the CCM.

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

Scroll down until you find the section that starts with **<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" />
```

The line that starts with SSLCipherSuite= lists the ciphers that are allowed and not allowed.

At the end of each of those lines add: **!3DES:!IDEA**

After you start Tomcat, 3DES and IDEA will no longer be used and so the Nmap scan will no longer report any warnings.

> **Note**: This workaround has not been tested for compatibility and some users might no longer be able to connect to the CCM User Interface (UI). Users with Windows XP and those that run IE v8 might not be able to connect anymore. However, it has not been tested.