توضح NMAP أن CCM عرضة لهجوم SWEET32

المحتويات

المقدمة

يصف هذا المستند مشكلة حيث تظهر NMAP أن مدير المكالمات (CCM) من Cisco قابل لهجوم SWEET32.

المشكلة

عندما تقوم بتشغيل NMAP 4.70+، ستري رسائل تحذيرية حول المعايار الثلاثي لتشفير البيانات (3DES) وفكرة تظهر أنه عرض ل SWEET32.

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

تم العثور على تشفيرات الأسبوع 64 بت قابلة لهجوم يعرف باسم Sweet32. ستحتوي الإصدارات الجديدة من NMAP على فحص لمعرفة ما إذا تم تمكين أي شفرة قابلة للتأثر. ولهذا السبب، يعرض تشغيل مسح NMAP على CCM هذا التحذير:

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

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

الحل

لا تتعلق هذه المشكلة مباشرة ب CloudCenter، ولكن خادم Tomcat الذي يستخدمه CloudCenter. وتجدر الإشارة إلى أنه المسح الضوئي الذي أجرته "NMAP" لا ينص على أن الجهاز معرض للخطر. هناك الظاهري (VM) لهجوم، بل إنه ذكر فقط أنه يستخدم شفرة معرضة للهجوم الذي لا تقوم NMAP باختباره. تغييرات أخرى مطلوب أن تكون موجودة لكي ينجح هذا الهجوم.

تذكرة أساسية، تم إنشاء CORE-15086 في لتعقب هذا الأمر. لا يزال الحل قيد المعالجة ويتم تحديث إصدار OpenSSL 1.1.0+ الذي سيقوم بدوره بتصحيح الخلل.

صرحت Engineering أنه يمكن تجاهل رسالة الخطأ بشكل آمن، ومع ذلك، يوجد حل بديل إذا لزم الأمر.

القشرة الآمنة (SSH) في CCM.

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

قم بالتمرير لأسفل حتى تجد المقطع الذي يبدأ ب **<منفذ الموصل="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" />
```

يسرد السطر الذي يبدأ ب SSLCipherSuite= الشفرات المسموح بها وغير المسموح بها.

في نهاية كل سطر من هذه الأسطر يضاف: **!3DES:!IDEA**

بعد بدء تشغيل Tomcat، لن يتم إستخدام 3DES و IDEA بعد الآن، وبالتالي لن يقوم Nmap بالمسح الضوئي بالإبلاغ عن أية تخذيرات.

> **ملاحظة**: لم يتم إختبار هذا الحل البديل للتوافق وقد لا يعود بإمكان بعض المستخدمين الاتصال بواجهة مستخدم CCM (UI). قد يتعذر على المستخدمين الذين لديهم نظام التشغيل Windows XP وأولئك الذين يقومون بتشغيل IE V8 الاتصال بعد الآن. غير أنه لم يتم إختباره.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).