أستكشاف أخطاء FindSe وإصلاحها "SSLPirUnverifyException" للأدوات المضيفة على خوادم CA الموقعة

المحتويات

المقدمة

يصف هذا المستند خطوات أستكشاف أخطاء السيناريو وإصلاحها حيث يتم تحميل سلسلة شهادات موقعة من قبل المرجع المصدق (CA) إلى Finesse لخادم ويب خارجي يستضيف أداة ذكية ولكن الأداة الذكية تفشل في التحميل عند تسجيل الدخول إلى Finesse وترى الخطأ "sslpIrUnverifiedException".

تمت المساهمة من قبل جيني شوينسبيرجر، مهندس مركز المساعدة الفنية من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شهادات SSL
- إدارة فايننس
- إدارة خادم Windows
- تحليل التقاط الحزمة باستخدام Wireshark

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- Unified Contact Center Express (UCCX) 11.x
- Finesse 11.x

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

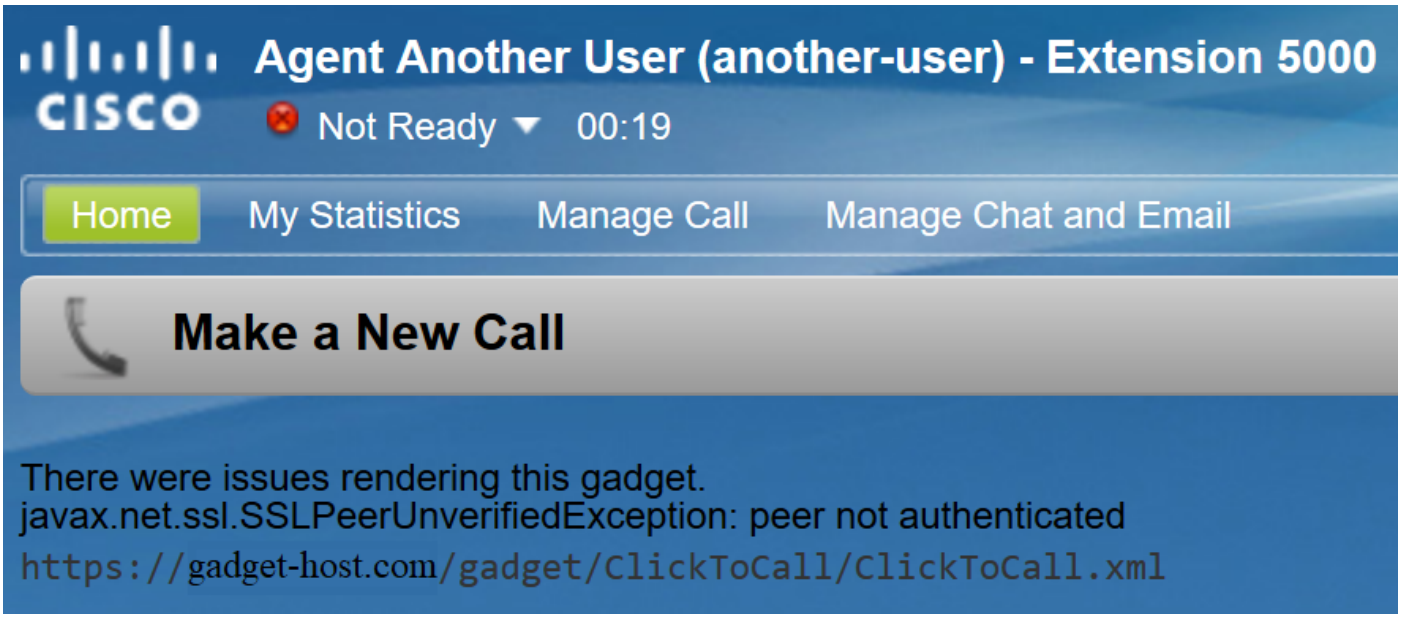
معلومات أساسية

هذه هي الظروف التي قد يحدث فيها الخطأ:

- افترض تحميل سلسلة الشهادات الموثوق بها إلى Finesse
- تأكد من إعادة تشغيل الخوادم/الخدمات الصحيحة
- افترض أنه تمت إضافة الأداة الذكية إلى تخطيط Finesse باستخدام عنوان URL لـ HTTPS وأن عنوان URL يمكن الوصول إليه

هذا هو الخطأ الذي تم ملاحظته عند تسجيل العميل الدخول إلى Finesse:

"كانت هناك مشكلات في عرض هذه الأداة الذكية. javax.net.ssl.SSLPirUnverifiedException: لم تتم مصادقة النظير"



مشاكل

السيناريو 1: يقوم الخادم المضيف بالتفاوض على قوائم التحكم في الوصول (TLS) غير الآمنة

عند قيام Finesse Server بطلب اتصال بالخادم المضيف، تعلن Finesse Tomcat عن قائمة بتشفير التشفير التي تدعمها.

ال يتم دعم بعض التشفير بسبب الثغرات الأمنية،

إذا قام الخادم المضيف بتحديد أي من هذه الشفرات، يتم رفض الاتصال:

- TLS_DHE_RSA_WITH_AES_256_cbc_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

من المعروف أن هذه المشفرات تستخدم مفاتيح Diffie-hellman سريعة الزوال عند التفاوض

على الاتصال، كما أن قابلية تأثر Logjam تجعل من هذه الخيارات خيارا سيئا لاتصالات TLS.

اتبع عملية مصافحة TLS في التقاط الحزمة لمعرفة أي تشفير يتم التفاوض عليه.

1. تقدم Finesse قائمة المشفرات المدعومة الخاصة بها في خطوة **Client Hello**:

```
▼ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 67
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 63
      Version: TLS 1.0 (0x0301)
    ▶ Random: 5cacb293b5efdb4cf1bb34464d7de9f5060b00a9beb81d29…
      Session ID Length: 0
      Cipher Suites Length: 24
    ▼ Cipher Suites (12 suites)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
        Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
        Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
        Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
```

2. لهذا الاتصال **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** تم إختياره بواسطة الخادم المضيف أثناء خطوة **Server Hello** لأن هذا أعلى في قائمته للشفرات المفضلة.

```
TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 2557
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.0 (0x0301)
    Random: 5cacb292c4d7183627f620a066f9b6ce6460dcb849b59cae…
    Session ID Length: 32
    Session ID: 4c290000ce66098cc994a33e193b0da1244cb9f083f69c26…
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Compression Method: null (0)
    Extensions Length: 5
    Extension: renegotiation_info (len=1)
  Handshake Protocol: Certificate
  Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 1032
    Diffie-Hellman Server Params
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
```

3. ترسل Finesse تنبيهًا فادحًا وتضع حدًا للاتصال:

```
TLSv1 Record Layer: Alert (Level: Fatal, Description: Internal Error)
  Content Type: Alert (21)
  Version: TLS 1.0 (0x0301)
  Length: 2
  Alert Message
```

الحل

لمنع إستخدام هذه الشفرات، يجب تكوين خادم الاستضافة لمنح هذه الشفرات أولوية منخفضة، أو يجب إزالتها من قائمة الشفرات المتاحة بالكامل. يمكن القيام بذلك على Windows Server باستخدام محرر نهج مجموعة Windows (gpedit.msc).

ملاحظة: لمزيد من التفاصيل حول تأثير Logjam في Finesse واستخدام GPEDIT، راجع:

السيناريو 2: تحتوي الشهادة على خوارزمية توقيع غير مدعومة

يمكن لجهات ترخيص Windows Server إستخدام معايير توقيع أحدث لتوقيع الشهادات. حتى أنه يوفر قدرا أكبر من الأمان مقارنة بتقييم أنظمة التشغيل SHA، فإن تبني هذه

المعايير خارج منتجات Microsoft منخفض ومن المحتمل أن يواجه المسؤولون مشاكل تتعلق بقابلية التشغيل البيني.

تعتمد Finesse Tomcat على موفر أمان SunMSCAPI من Java لتوفير الدعم لمختلف خوارزميات التوقيع ووظائف التشفير التي تستخدمها Microsoft. تدعم جميع الإصدارات الحالية من Java (1.7 و 1.8 و 1.9) خوارزميات التوقيع هذه فقط:

- MD5withRSA
- MD2withRSA
- NONEwithRSA
- SHA1withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

لتأكيد إنها لفكرة جيدة أن تتحقق من إصدار Java الذي يتم تشغيله على خادم Finesse الخوارزميات التي يتم دعمها في هذا الإصدار. يمكن التحقق من الإصدار من الوصول الجذر باستخدام هذا الأمر: **Java -version**

```
Using username "root".
Last login: Tue Apr 16 13:11:00 2019 from
[root@uccx12pub ~]# java -version
java version "1.7.0_181"
OpenJDK Runtime Environment (rhel-2.6.14.8.el6_9-i386 u181-b00)
OpenJDK Server VM (build 24.181-b00, mixed mode)
[root@uccx12pub ~]#
```

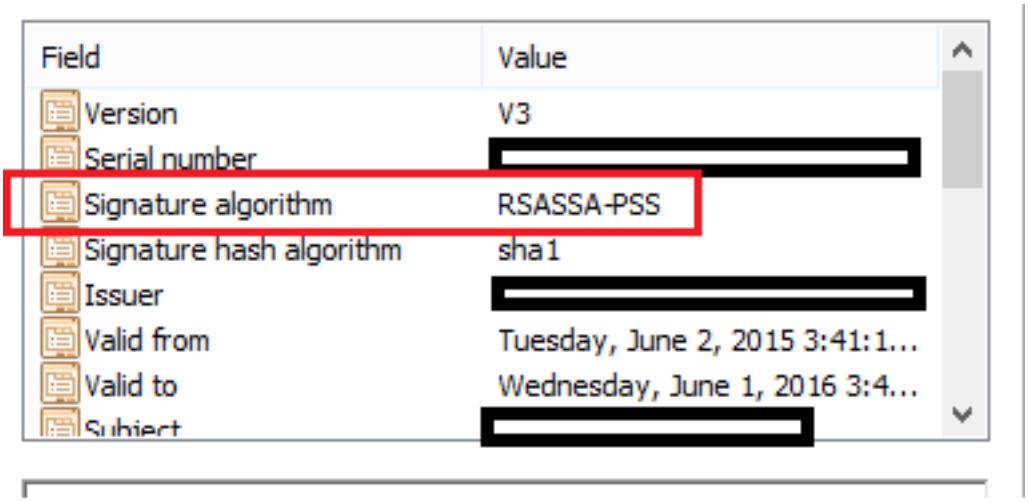
> **ملاحظة**: لمزيد من التفاصيل حول موفر Java SunMSCAPI، ارجع إلى https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html#SunMSCAPI

إذا تم توفير شهادة مع توقيع آخر غير المذكور أعلاه، فلن يتمكن Finesse من إستخدام الشهادة لإنشاء اتصال TLS بخادم الاستضافة. يشمل ذلك الشهادات الموقعة بنوع توقيع مدعوم ولكن تم إصدارها من قبل هيئات التصديق التي لديها شهاداتها الوسيطة والجذرية موقعة مع شيء آخر.

إذا نظرت إلى التقاط حزمة، يقوم Finesse بإغلاق الاتصال بخطأ "تنبيه قاتل: الشهادة غير معروفة"، كما هو موضح في الصورة.

```
Secure Sockets Layer
⊟ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
    Content Type: Alert (21)
    Version: TLS 1.2 (0x0303)
    Length: 2
  ⊟ Alert Message
      Level: Fatal (2)
      Description: Certificate Unknown (46)
```

عند هذه النقطة من الضروري التحقق من الشهادات المقدمة من قبل الخادم المضيف والبحث عن خوارزميات توقيع غير مدعومة. من الشائع أن ترى **RSA-PSS** كخوارزمية التوقيع الإشكالي:



إذا تم توقيع أي شهادة في السلسلة مع RSASSA-PSS، يفشل الاتصال. في هذه الحالة يظهر التقاط الحزمة أن المرجع المصدق الجذر يستخدم RSAa-PSS لشهادته الخاصة:

```
Certificates (3906 bytes)
  Certificate Length: 1728
  Certificate: 308206bc308205a4a003020102021374000000243b805da9... (id-at-commonName=[redacted]
    signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: e6230df257be9d34c0f57bc2f88c081c4186aaad092c8155...
  Certificate Length: 1114
  Certificate: 308204563082033ea003020102021316000000a93cd17d6... (id-at-commonName=[redacted]Issuing Authority[redacted]
    signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: 889be6a1125c758cd0009b392d3b90a69b64546dcee09c84...
  Certificate Length: 1055
  Certificate: 3082041b308202cfa00302010202107b70dbb7c2760da74f... (id-at-commonName=[redacted]Root CA [redacted]
    signedCertificate
    algorithmIdentifier (id-RSASSA-PSS)
      Algorithm Id: 1.2.840.113549.1.1.10 (id-RSASSA-PSS)
      RSASSA-PSS-params
      Padding: 0
      encrypted: d8e9151adc76b4e55f9277fce916613ce26199e3b50dcb54...
```

الحل

لحل هذه المشكلة، يجب إصدار شهادة جديدة من موفر CA يستخدم نوع واحد فقط من أنواع توقيعات SunMSCAPI المدعومة المدرجة عبر سلسلة الشهادات بالكامل كما هو موضح مسبقا.

ملاحظة: لمزيد من التفاصيل حول خوارزمية توقيع RSA-PSS، راجع https://pkisolutions.com/pkcs1v2-1rsassa-pss/

ملاحظة: يتم تعقب هذه المشكلة في الخلل CSCve79330

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).