أستكشاف أخطاء CommPilot "؛SSL_ERROR_NO_CIPHER_OVERLAP" وإصلاحها؛

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين BroadWorks واستكشاف أخطائها وإصلاحها لتجنب خطأ "SSL_ERROR_NO_CIPHER_OVERLAP".

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال BroadWorks منصة.

معلومات أساسية

تكوين BroadWorks

بالنسبة للإصدارات 22 من Broadworks والإصدارات الأحدث، تكون البروتوكولات والشفرات القابلة للتكوين عبر واجهة سطر الأوامر (CLI) من خلال السياقات التي يتم رؤيتها على مستويات تكوين مختلفة.

```
'Interface/Port specific - low level'
CLI/Interface/Http/HttpServer/SSLSettings/Protocols
CLI/Interface/Http/HttpServer/SSLSettings/Ciphers

'All interfaces - mid level'
CLI/Interface/Http/SSLCommonSettings/Protocols
CLI/Interface/Http/SSLCommonSettings/Ciphers

'Generic system level - high level'
CLI/System/SSLCommonSettings/JSSE/Protocols
CLI/System/SSLCommonSettings/JSSE/Ciphers
```

يشير السياق المسمى SSLCommonSettings إلى عنصر أقل تحديدا من تسلسل SSL الهرمي وسياق يسمى SSLettings إلى عنصر أكثر تحديدا من التدرج الهرمي.

مثال للمختبر الوظيفي

التكوين

تكوين منخفض المستوى مرتبط باولاجهة والمنفذ الخاصين دون تشفير معرف:

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.1
TLSv1.2
TLSv1

CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443
Cipher Name
=============

0 entry found.
```

التحقق

تحقق من التكوين باستخدام curl :

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_RSA_WITH_AES_256_CBC_SHA256 <-----
* Server certificate:
* subject:
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX
* start date: Apr 04 20:39:56 2022 GMT
* expire date: Apr 04 20:39:56 2023 GMT
* common name: *.calo.cisco.com
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Tecolutla,ST=Veracruz,C=MX
>GET / HTTP/1.1
>User-Agent: curl/7.29.0
>Host: 172.16.30.146
>Accept: */*
>
<HTTP/1.1 302 Found
```

هنا تم الاتصال بنجاح عبر TLSv1.2 بشفرة TLS_RSA_WITH_AES_256_CBC_SHA256.

تدقيق الاتصال

للتحقق من البروتوكولات والشفرات التي تم قبولها:

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 04:26 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.00013s latency).
PORT STATE SERVICE VERSION
443/tcp open ssl/https?
| ssl-enum-ciphers:
| TLSv1.0:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.1:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA256 - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
|_ least strength: strong
```

مثال عملي عن خطأ

المشكلة

حدث خطأ - "SSL_ERROR_NO_CIPHER_OVERLAP" عبر المستعرض.

```
# curl -v https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
```

```
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt
CApath: none
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0 curl: (35) Cannot communicate securely with peer: no common encryption
algorithm(s).
```

التكوين

التكوين منخفض المستوى المرتبط بالواجهة والمنفذ المحددة باستخدام بروتوكول TLSv1.2 الذي تم تعيينه باستخدام مجموعة TLSv1.0 Cipher TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256:

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.2

CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
=====================================
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
```

التحقق

تحقق من التكوين باستخدام curl :

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0
curl: (35) Cannot communicate securely with peer: no common encryption algorithm(s).
```

تدقيق الاتصال

للتحقق من البروتوكولات والشفرات التي تم قبولها:

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:31 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000049s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
|_ TLSv1.2: No supported ciphers found
```

من نتائج الأداة، يلاحظ أن بروتوكول TLSv1.2 متاح ولكن لا توجد شفرات مدعومة.

قرار

احذف تشفير TLSv1.1 الموجود ضمن **CLI/Interface/Http/SSLCommonSettings/Ciphers** ، ثم افتح جميع شفرات TLSv1.2 مرة أخرى (أو أضف تشفير TLSv1.2).

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.2

CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443
Cipher Name
=============
0 entry found.

CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
=============
0 entry found.
```

التحقق من القرار

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 <-----
* Server certificate:
* subject:
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX
* start date: Apr 04 20:39:56 2022 GMT
* expire date: Apr 04 20:39:56 2023 GMT
* common name: *.calo.cisco.com
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Tecolutla,ST=Veracruz,C=MX
>GET / HTTP/1.1
>User-Agent: curl/7.29.0
>Host: 172.16.30.146
>Accept: */*
>
<HTTP/1.1 302 Found

$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:44 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000063s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - strong
```

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).