أستكشاف أخطاء تحديث موجز معلومات الأمان وإصلاحها على مركز إدارة Firepower

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء تحديثات موجز ويب الذكاء الأمان وإصلاحها.

الخلفية

يتكون موجز المعلومات للاستخبارات الأمنية من قوائم متعددة محدثة بشكل منتظم لعناوين IP ذات سمعة سيئة، كما هو محدد بواسطة مجموعة Cisco Talos Security Intelligence and Research Group (Talos). من المهم الحفاظ على تحديث موجز ويب الذكاء بشكل منتظم حتى يمكن لنظام Cisco Firepower إستخدام المعلومات الحديثة لتصفية حركة مرور الشبكة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة FireSIGHT التابع لشركة Cisco
- تغذية المعلومات الإستخباراتية الأمنية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مركز إدارة Cisco Firepower الذي يشغل الإصدار 5.2 من البرنامج أو إصدار أحدث.

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.

المشكلة

يحدث فشل في تحديث موجز ويب لمعلومات الأمان. يمكنك التحقق من الفشل إما من خلال واجهة المستخدم الرسومية (GUI) للويب أو واجهة سطر الأوامر (يتم شرحها أكثر في الأقسام التالية).

تحقق من المشكلة من واجهة المستخدم الرسومية (GUI) للويب

عند حدوث فشل في تحديث موجز ويب لذكاء الأمان، يعرض مركز إدارة Firepower تنبيهات السالمة.

دقق المشكلة من ال CLI

دخلت in order to حددت السبب الجذر للتحديث إخفاق مع الأمنية ذكاء موجز، هذا أمر دخل ال CLI من ال firepower إدارة مركز:

```
admin@Sourcefire3D:~$ cat /var/log/messages
```

ابحث عن أي من هذه التخييرات في الرسائل:

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

الحل

أتمت هذا steps in order to تحريت المشكلة:

1. تحقق من أن intelligence.sourcefire.com الموقع نشط. انتقل إلى https://intelligence.sourcefire.أدخل متصفح.
2. الوصول إلى واجهة سطر الأوامر (CLI) لمركز إدارة FirePOWER من خالل Secure Shell (SSH).
3. بينغ intelligence.sourcefire.com من مركز إدارة Firepower:

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verifyyou receive an output similar
   to this:

   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ifyou do not receive a
   response similar to that shown, then you can have an outbound connectivity issue, or you do
   not have a route to intelligence.sourcefire.com.
   ```
4. حل اسم المضيف ل intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com
```

تحقق من تلقي إستجابة مماثلة لهذا:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

ملاحظة: يستخدم المنتج الأصلي DNS الخاص بـ (DNS) في حالة توجيه أسماء المجالات الخارجية. **يجب عليك** التحقق من إعدادات DNS التي تم تكوينها في **النظام > محلي > التكوين**، ضمن قسم **Network**. إذا لم تتلق إستجابة مماثلة لتلك الموضحة، فتأكد من صحة إعدادات DNS.**تحذير**: يستخدم الخادم مخطط عنوان IP دائري للتوازن بين الأحمال والتسامح مع الأخطاء. لذلك، يمكن أن تتغير عناوين IP، وتوصي Cisco بتكوين جدار الحماية باستخدام **CNAME** بدلا من عنوان IP.

5. تحقق من الاتصال بـ intelligence.sourcefire.com باستخدام برنامج Telnet:

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

تحقق من إستلام مخرجات مماثلة لهذا:

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

ملاحظة: إذا كان بإمكانك إكمال الخطوة الثانية بنجاح ولكن يتعذر عليك إستخدام برنامج Telnet في **intelligence.sourcefire.com** عبر المنفذ 443، يمكنك الحصول على قاعدة جدار حماية تمنع المنفذ 443 الصادر من أجل intelligence.sourcefire.com.

6. انتقل إلى **النظام > محلي > التكوين** وتحقق من إعدادات الوكيل الخاصة بـ **Manual Proxy** في إطار قسم **Network**.
ملاحظة: إذا قام هذا الوكيل بفحص طبقة مآخذ التوصيل الآمنة (SSL)، فيجب عليك وضع قاعدة تجاوز تجاوز الوكيل لـ **intelligence.sourcefire.com.**

7. قم بالاختبار إذا كان بإمكانك إجراء HTTP GET طلب ضد intelligence.sourcefire.com:

```
admin@Firepower:~sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
```

```
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

ملاحظة: الوجه المبتسم في نهاية curl تشير مخرجات الأمر إلى اتصال ناجح.**ملاحظة**: إذا كنت تستخدم وكيل، فإن curl يتطلب الأمر اسم مستخدم. الأمر **curl -u <user> -vvk** https://intelligence.sourcefire.com. وبالإضافة إلى ذلك، بعد إدخال الأمر، تتم مطالبتك بإدخال كلمة مرور الوكيل.

8. تحقق من حركة مرور HTTPS المستخدمة لتنزيل موجز وبيانات الأمان التي تمر من خلال جهاز فك تشفير SSL. للتحقق من عدم حدوث فك تشفير SSL، تحقق من علامات شهادة الخادم في الإخراج من الخطوة 6. إذا لم تتطابق شهادة الخادم مع ما هو معروض في المثال التالي، يمكن الحصول على جهاز فك تشفير SSL الذي يستردّ الشهادة. إذا مرت حركة المرور عبر فك تشفير SSL، فيجب عليك تجاوز جميع حركة المرور التي تنتقل إليها intelligence.sourcefire.com.

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
```

```
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

ملاحظة: يجب تواجد فك تشفير SSL لموجز معلومات الأمان الذكية لأن جهاز فك تشفير SSL يرسل إلى مركز إدارة Firepower شهادة غير معروفة في مصافحة SSL. لم يتم توقيع الشهادة المرسلة إلى مركز إدارة Firepower من قبل مرجع مصدق موثوق به ل Sourcefire، لذا فإن الاتصال غير موثوق به.

معلومات ذات صلة

- [تلقائيمايتيتش فشل تنزيل تحديث مركز إدارة FirePOWER]
- [عناوين الخادم المطلوبة لعمليات الحماية المتقدمة من البرامج الضارة (AMP)]
- [منافذ الاتصال المطلوبة لتشغيل نظام FirePOWER]
- [الدعم التقني والمستندات - Cisco Systems]

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).