تعرف على برنامج الاستجابة الأولى (إصدار جدار الحماية الآمن)

المحتويات

المقدمة

يصف هذا المستند إستخدام برنامج المستجيب الأول وتنفيذه ل Cisco Secure Firewall.

المتطلبات الأساسية

المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

يعتمد هذا المستند على منتجات جدار الحماية الآمن من Cisco.

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 فهم للتأثير المحتمل لأي أمر.

معلومات أساسية

تم إنشاء برنامج المستجيب الأول بواسطة TAC لتسهيل وتسريع توفير بيانات التشخيص للحالات المفتوحة. هناك مكونان رئيسيان يشكلان البرنامج:

البريد الإلكتروني التلقائي

يتم إرسال هذا البريد الإلكتروني في بداية الحالة مع إرشادات حول كيفية تجميع بيانات التشخيص وتحميلها لتحليل TAC. هناك العديد من التقنيات التي تستفيد من هذا النظام، ويتم تعيين كل بريد إلكتروني على "التقنية" و"التقنية الفرعية" التي يتم إختيارها عند إنشاء الحالة.

نص تنفيذي / أوامر

ولكل عملية تنفيذ لبرنامج "المستجيب الأول" طريقته الفريدة لمعالجة جمع البيانات وتوصيلها. يستخدم تنفيذ جدار الحماية الآمن برنامج FirePOWER.py Python المرفق من TAC لتحقيق ذلك. تقوم عملية البريد الإلكتروني المؤتمتة بإنشاء أمر سطر واحد، قبل جدار الأجهزة (CLI) سطر الأوامر هذه الحالة المحددة، يمكن نسخ ولصقه في واجهة فريد لهذه الحالة المحددة، يمكن نسخ ولصقه في واجهة سطر الأوامر (CLI) لأجهزة جدار الحماية الآمنة للتشغيل.

سبب هذا البريد الإلكتروني

هناك تقنيات معينة تم تمكينها لبرنامج المستجيب الأول. وهذا يعني أنه في كل مرة يتم فتح حالة دعم جديدة، يتم إرسال بريد إلكتروني للمستجيب الأول. إذا تلقيت رسالة بريد إلكتروني من أول المستجيبين ولم تعتقد أن طلب البيانات مهم، فيرجى عدم تجاهل الاتصال.

في حالة إستخدام جدار الحماية الآمن، يقتصر برنامج الاستجابة الأولى على برنامج الدفاع عن تهديد FirePOWER (FTD). إذا قمت بتشغيل قاعدة تعليمات برمجية لأجهزة الأمان المعدلة (ASA)، فيرجى تجاهل هذه الرسالة الإلكترونية. ونظرا لأن هذين المنتجين يعملان على نفس الجهاز، فيالحظ بشكل عام أنه يتم إنشاء حالات ASA في مساحة تقنية جدار الحماية الآمن، التي تقوم بإنشاء رسالة البريد الإلكتروني للمستجيب الأول.

البريد الإلكتروني التلقائي

فيما يلي مثال على البريد الإلكتروني التلقائي الذي يتم إرساله كجزء من هذا البرنامج:

```
From: first-responder@cisco.com <first-responder@cisco.com>
```

```
Sent: Thursday, September 1, 2022 12:11 PM
To: John Doe <john.doe@cisco.com>
Cc: attach@cisco.com
Subject: SR 666666666 - First Responder Automated E-mail

Dear John,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution and the steps to collect them:

*** Troubleshoot File ***

* Connect to the device using SSH
* Issue the command expert, skip this step for FMC version 6.4.x and earlier
* Issue the command sudo su
* When prompted for the password, enter your password.
* For FMC 6.4 or FTD 6.7 and later issue the command
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

* For FMC 6.3 or FTD 6.6 and earlier issue the command
curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

For more information on what this command does, or to understand why you are receiving this e-
mail - please refer to
<LINK_TO_THIS_ARTICLE>

For 6.3 and earlier versions we recommend confirming cxd.cisco.com resolves to <CURRENT_CXD_IP1>
or
<CURRENT_CXD_IP2>. Furthermore, we recommend validating the SHA checksum of the file by running
url -s -k https://cxd.cisco.com/public/ctfr/firepower.py | shasum which should output
<CURRENT_SHA>.

If you are unable to upload troubleshooting files (or would prefer not to), please let us know
what
hardware and software version ou are running if you have not already.

Sincerely, First Responder Team
```

تم تقسيم رسائل البريد الإلكتروني المؤتمتة الخاصة ببرنامج المستجيب الأول إلى جزأين معروفين باسم كتلة المقدمة وكتلة طلب البيانات.

كتلة المقدمة

كتلة المقدمة هي سلسلة ثابتة يتم تضمينها في كل بريد إلكتروني للمستجيب الأول. فهذه الجملة الاستهلالية تفيد سوى في توفير سياق لكتل (كتل) طلب البيانات. هنا مثال على كتلة مقدمة:

```
Dear <NAME>,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution
and the steps to collect them:
```

كتلة طلب البيانات

تمثل كتل طلب البيانات جوهر برنامج المستجيب الأول. كل مجموعة هي مجموعة محددة مسبقا من الخطوات لجمع البيانات لتقنية معينة. كما هو مذكور في قسم **معلومات الخلفية**، يتم تعيين كل كتلة طلب بيانات على تقنية معينة. هذه هي نفس التقنية التي تم إختيارها لفتح حالة دعم. عادة ما يحتوي البريد الإلكتروني التلقائي على كتلة طلب بيانات واحدة. ومع ذلك، إذا كانت التقنية المحددة تحتوي على أكثر من كتلة طلب بيانات واحدة معينة إليها، فسيتم تضمين طلبات بيانات متعددة في البريد الإلكتروني. فيما يلي تنسيق مثال لكتلة "طلب البيانات" مع طلبات بيانات متعددة:

```
*** <REQUEST NAME 1> ***

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

على سبيل المثال، في حالة "جدار الحماية الآمن"، غالبا ما يتم تضمين العديد من كتل طلب البيانات عندما يتم رفع طلب للمساعدة في مشاكل الوصول عن بعد إلى شبكة VPN (RA-VPN) مع "الدفاع عن تهديد الطاقة النارية (FTD)" نظرا لأن تقنية VPN تحتوي أيضا على كتلة طلب بيانات تم تعيينها تم تكوينها للمساعدة في تجميع حزم DART.

أمر وليد

بالنسبة لحالة إستخدام جدار الحماية الآمن على وجه التحديد، يتم إنشاء أمر سطر واحد فريد لكل حالة كجزء من البريد الإلكتروني التلقائي. فيما يلي تصنيف لتركيبة أمر السطر الواحد:

```
# curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t aBcDeFgHiJkLmNoP --auto-upload &
    1   2  3  4                     5                          6    7            8                 9                   10         11
```

1. يتم إستخدام الأمر curl لتنزيل أحدث إصدار من برنامج Firepower.py النصي
2. علامة **-k** خيار للغير لتجاهل أخطاء الشهادة أثناء الاتصال.
3. العلم **-** هو خيار لتعمل Curl في الوضع الصامت. يستخدم هذا لمنع مخرجات التجعد العادية لأنها مشوشة.
4. علامة **-S** خيار لعلامة التجعد لإظهار الأخطاء. يتم إستخدام هذا لإجبار التجعد على الاستمرار في إظهار أخطاء الإخراج حتى مع تمكين الخيار الصامت.
5. عنوان URL الذي يتم فيه إستضافة أحدث إصدار من Firepower.py Script. يرشد هذا المسار أمر التجعد لسحب آخر نص تنفيذي ليتم تشغيله.
6. هذا أنبوب لينوكس، الذي يقوم بتمرير مخرجات الأمر الالتفاف (محتويات نص بيثون) إلى بيان تنفيذ في الخطوة التالية.
7. في هذه الخطوة، يتم إستدعاء ثنائي بايثون على الجهاز مع "-" إضافي. وهذا يرشد بايثون ان المصدر مأخوذ من الصل (لأن محتويات النص تنقل من التجعد).
8. علامة **-c** هي وسيطة إدخال للبرنامج النصي Firepower.py، والتي تشير إلى رقم الحالة الذي يجب تحميل البيانات إليه. قيمة 6666666666 بعد هذا الخيار هي مثال رقم الحالة.
9. علامة **-t** هي وسيطة إدخال للبرنامج النصي firepower.py، والتي تشير إلى رمز مميز (كلمة مرور) تم إنشاؤه لهذه الحالة الخاصة. قيمة aBcDeFgHiJkLmNoP بعد هذا الخيار هي رمز المثال المميز لهذه الحالة.
10. تعد علامة **—التحميل التلقائي** وسيطة خاصة للبرنامج النصي firepower.py، والذي يشير إلى البرنامج النصي الذي سيتم تشغيله في وضع التشغيل التلقائي. يمكن العثور على مزيد من المعلومات حول هذا في القسم الخاص بالبرنامج النصي.
11. إن **&** يرشد هذا الأمر بأكمله أن يعمل في الخلفية، مما يسمح للمستخدم بمواصلة

التفاعل مع قشرتهم أثناء تنفيذ النص التنفيذي.

ملاحظة: يلزم وجود علامة -k لأي إصدار من FMC قبل الإصدار 6.4 وأي إصدار من FTD قبل الإصدار 6.7 نظرا لأن الشهادة الجذر المستخدمة من قبل CXD لم تكن موثوق بها من قبل أجهزة FirePOWER حتى الإصدار 6.4 من FMC والإصدار 6.7 من FTD، مما يتسبب في فشل التحقق من الشهادة.

برنامج Firepower.py Script

الهدف الرئيسي للبرنامج النصي هو إنشاء حزمة تشخيص وتحميلها من جهاز الحماية من النار المشار إليه باسم "أستكشاف الأخطاء وإصلاحها". إنشاء ملف أستكشاف الأخطاء وإصلاحها هذا، ويدعو البرنامج النصي firepower.py بواسطة البرنامج النصي SF_troubleshooting.pl المدمج المسؤول عن إنشاء هذه الحزمة. هذا هو نفس البرنامج النصي الذي يتم استدعاؤه عندما يطلب أستكشاف أخطاء وإصلاحها من واجهة المستخدم الرسومية (GUI). بالإضافة إلى ملف أستكشاف الأخطاء وإصلاحها، يتمتع البرنامج النصي أيضا بالقدرة على تجميع بيانات تشخيصية أخرى غير مضمنة كجزء من حزمة أستكشاف الأخطاء وإصلاحها. وفي الوقت الحالي، فإن البيانات الإضافية الوحيدة التي يمكن جمعها هي الملفات الأساسية ولكن يمكن توسيع نطاق هذه البيانات في المستقبل إذا دعت الحاجة إلى ذلك. يمكن تشغيل البرنامج النصي إما في الوضع "Automation" أو "Interactive":

أتمتة

يتم تمكين هذا الوضع عند إستخدام الخيار "—التحميل التلقائي" عند تشغيل البرنامج النصي. يقوم هذا الخيار بتعطيل موجهات الأوامر التفاعلية وتمكين مجموعة الملفات الأساسية وتحميل البيانات تلقائيا إلى الحالة. يتضمن الأمر أحادي السطر الذي تم إنشاؤه بواسطة البريد الإلكتروني التلقائي خيار "—التحميل التلقائي".

تفاعلي

هذا هو الوضع الافتراضي لتشغيل البرنامج النصي. في هذا الوضع، يتلقى المستخدم مطالبات لتأكيد ما إذا كان سيتم جمع بيانات تشخيصية إضافية مثل الملفات الأساسية أم لا. بغض النظر عن وضع التنفيذ، فإن المخرجات ذات المعنى تطبع على الشاشة وتسجل في ملف سجل للتشغيل إلى تدفق تنفيذ البرامج النصية. يتم توثيق البرنامج النصي نفسه بشكل مكثف من خلال تعليقات التعليمات البرمجية في السطر ويمكن تنزيله / مراجعته على https://cxd.cisco.com/public/ctfr/firepower.py.

الإخراج المتوقع من البرنامج النصي

فيما يلي مثال على تنفيذ ناجح للنص:

```
root@ftd:/home/admin# curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c
666666666 -t aBcDeFgHiJkLmNoP --auto-upload &
[1] 26422
root@ftd:/home/admin#
`/var/common/first_responder_notify` successfully uploaded to 666666666
Running sf_troubleshoot.pl command to create a troubleshoot file...
Troubleshoot file successfully generated at /ngfw/var/common/results-08-30-2022--135014.tar.gz
Attempting to upload troubleshoot to case...
##########################################################################################
############################ 100.0%
`/ngfw/var/common/results-08-30-2022--135014.tar.gz` successfully uploaded to 666666666
```

```
Found the following core files:
(0 B) - /ngfw/var/common/core_FAKE1.gz
(0 B) - /ngfw/var/common/core_FAKE2.gz
(0 B) - /ngfw/var/common/core_FAKE3.gz
Successfully created /ngfw/var/common/cores_666666666-1661867858.tar.gz
Attempting core file upload...
################################################################################################################
############################## 100.0%
`/ngfw/var/common/cores_6666666660-1661867858.tar.gz` successfully uploaded to 666666666
FINISHED!
```

الرجاء ملاحظة أن مثال الإخراج هذا يتضمن عمليات تحميل الملفات الأساسية. في حالة عدم وجود ملفات أساسية على الجهاز، يتم إرسال رسالة "No core files found. Skipping core file processing" تقدم بدلا من ذلك.

المشكلات الشائعة

فيما يلي بعض القضايا المشتركة التي يمكنك تجربتها (من أجل معالجتها / تنفيذها):

إعادة كتابة أمان البريد الإلكتروني / عنوان URL

غالبا ما تتم ملاحظة أن المستخدم النهائي لديه مستوى ما من أمان البريد الإلكتروني الذي يعيد كتابة عنوان URL. يؤدي هذا إلى تغيير الأمر أحادي السطر الذي يتم إنشاؤه كجزء من البريد الإلكتروني التلقائي. يؤدي هذا إلى فشل التنفيذ نظرا لإعادة كتابة URL الخاص بسحب البرنامج النصي وعدم صلاحيته. هنا مثال من الموقع واحد خط أمر:

```
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &
```

الخطوات اللازمة للحل

إذا كان عنوان URL الموجود في الأمر من البريد الإلكتروني غير https://cxd.cisco.com/public/ctfr/firepower.py"، فمن المحتمل أن تتم إعادة كتابة عنوان URL أثناء النقل. لإصلاح هذه المشكلة، بساطة استبدلت ال URL قبل أن نقوم بتشغيل الأمر.

فشل DNS

غالبا ما يظهر هذا الخطأ المجدد عندما يكون الجهاز غير قادر على حل عنوان URL لتنزيل البرنامج النصي:

```
curl: (6) Could not resolve host: cxd.cisco.com
```

الخطوات اللازمة للحل

لحل هذه المشكلة، الرجاء التحقق من إعدادات DNS على الجهاز للتأكد من قدرته على حل URL بشكل صحيح للمتابعة.

فشل في فتح / إنشاء ملف سجل

أحد الأشياء الأولى التي يحاول البرنامج النصي القيام بها هو إنشاء ملف سجل (أو فتحه، إذا كان موجودا بالفعل) باسم First-responder.log في دليل العمل الحالي. في حالة فشل هذه

العملية، يظهر خطأ يشير إلى وجود مشكلة بسيطة في الإذن:

```
Permission denied while trying to create log file. Are you running this as root?
```

عند تنسيق هذه العملية، كل الأخطاء الأخرى تم تعريفها وطباعتها للشاشة بهذا التنسيق:

```
Something unexpected happened while trying to create the log file. Here is the error:
----------

----------
```

الخطوات اللازمة للحل

هذا الخطأ بسبب قيام البرنامج النصي كمستخدم إداري مثل "admin" أو "root".

فشل في فتح / كتابة ملف الإخطار

عند تنفيذ البرنامج النصي، تم إنشاء ملف من 0 بايت باسم "first_responder_notify" على النظام. ثم يتم تحميل هذا الملف إلى الحالة عند التشغيل التالي لهذا البرنامج. تمت كتابة هذا الملف إلى الدليل "/var/common". إذا كان المستخدم الذي يقوم بتنفيذ البرنامج النصي ليس لديه الأذونات الكافية لكتابة الملفات إلى هذا الدليل، فإن البرنامج النصي يعرض الخطأ:

```
Failed to create file -> `/var/common/first_responder_notify`. Permission denied. Are you
running as root?
```

الخطوات اللازمة للحل

هذا الخطأ بسبب قيام البرنامج النصي كمستخدم إداري مثل "admin" أو "root".

> **ملاحظة**: في حالة مواجهة خطأ تم قطع الاتصال، تم طباعة خطأ في كافة محتويات الشاشة "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". يمكن العثور على نص الاستثناء الكامل في First-responder.log.

فشل تأمين ملف sf_troubleshooting.pid

للتأكد من تشغيل عملية إنشاء واحدة فقط في وقت واحد، يحاول البرنامج النصي لإنشاء أستكشاف الأخطاء وإصلاحها تأمين ملف /var/sf/run/sf_troubleshoot.pid قبل المتابعة. إذا فشل البرنامج النصي في تأمين الملف، يظهر خطأ:

```
Failed to run the `sf_troubleshoot.pl` command - existing sf_troubleshoot process detected.
Please wait for existing process to complete.
```

الخطوات اللازمة للحل

معظم الوقت، يعني هذا الخطأ أن مهمة إنشاء مستقلة الاستكشاف الأخطاء وإصلاحها قيد التنفيذ بالفعل. في بعض الأحيان يكون هذه المستخدمين الذين ينفذون أمر السطر الواحد عن طريق الخطأ مرتين على التوالي. لإصلاح هذه المشكلة، انتظر انتهاء مهمة إنشاء أستكشاف الأخطاء وإصلاحها الحالية ثم حاول مرة أخرى لاحقا.

> **ملاحظة**: في حالة حدوث خطأ في البرنامج النصي SF_TROUBLESHOOTINGot.pl نفسه، يتم عرض هذا الخطأ على الشاشة **"Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error".** يمكن العثور على نص الاستثناء الكامل في **First-responder.log** .

تحميل المشاكل

هناك وظيفة تحميل مشتركة في البرنامج النصي مسؤولة عن جميع عمليات تحميل الملفات خلال تنفيذ البرامج النصية. هذه الدالة ببساطة عبارة عن برنامج تضمين يأخذ أي أخطاء تحدث أثناء التنفيذ، كرمز خطأ مترجم. في حالة فشل التحميل، يتم عرض هذا الخطأ على الشاشة:

```
[FAILURE] Failed to upload `/var/common/first_responder_notify` to 666666666. Please check the first-responder.log file for the full error
```

تحقق من ملف **First-responder.log** للاطلاع على الخطأ الكامل. بشكل نموذجي، يبدو ملف First-responder.log كما يلي:

```
08/29/2022 06:51:57 PM - WARNING - Upload Failed with the following error:
----------
Command '['curl', '-k', '--progress-bar',
'https://666666666:aBcDeFgHiJkLmNoP@cxd.cisco.com/home/',
'--upload-file', '/var/common/first_responder_notify']' returned non-zero exit status 6
----------
```

الخطوات اللازمة للحل

في هذه الحالة، أرجع Curl الخروج من 6 مما يعني **"فشل حل المضيف"**. هذا بسبب فشل DNS لحل اسم المضيف **cxd.cisco.com** . الرجاء الرجوع إلى وثائق الارتباط لفك ترميز أثناء محاولة حل المضيف المعروفة. أي حالات خروج غير معروفة.

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).