Informazioni sul programma First Responder (Secure Firewall Edition)

Sommario

Introduzione

Questo documento descrive l'utilizzo e l'implementazione del programma First Responder per Cisco Secure Firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Questo documento è basato sui prodotti Cisco Secure Firewall.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il programma First Responder è stato creato da TAC per semplificare e velocizzare la fornitura di dati diagnostici per i casi aperti. Il programma è costituito da due componenti principali:

Posta elettronica automatizzata

Questa e-mail viene inviata all'inizio della richiesta con istruzioni su come raccogliere e caricare i dati diagnostici per l'analisi TAC. Esistono diverse tecnologie che sfruttano questo sistema e ogni e-mail viene mappata sulla "Tecnologia" e sulla "Sottotecnologia" che vengono scelte al momento della creazione del caso.

Script/Comandi

Ogni implementazione del programma First Responder dispone di un proprio modo esclusivo per gestire la raccolta e la consegna dei dati. A tale scopo, l'implementazione Secure Firewall utilizza lo script firepower.py Python creato da TAC. Il processo di posta elettronica automatizzato genera un comando a riga singola, specifico per questo caso specifico, che può essere copiato e incollato nella CLI dei dispositivi Secure Firewall da eseguire.

Motivo dell'e-mail

Alcune tecnologie sono abilitate per il primo programma responder. Ciò significa che ogni volta che viene aperta una richiesta relativa a una di queste tecnologie abilitate, viene inviata una e-mail del primo responder. Se ricevi un'e-mail con il primo responder e non ritieni che la richiesta di dati sia rilevante, non esitare a ignorare la comunicazione.

Nel caso di utilizzo di Secure Firewall, il primo programma di risposta è limitato al software Firepower Threat Defense (FTD). Se si esegue una base di codice ASA (Adaptive Security Appliance), ignorare questa e-mail. Poiché i due prodotti vengono eseguiti sullo stesso hardware, si osserva generalmente che le richieste ASA vengono create nello spazio della tecnologia Secure Firewall, che genera l'e-mail del primo risponditore.

Posta elettronica automatizzata

Di seguito è riportato un esempio della posta elettronica automatizzata inviata come parte di questo programma:

```
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
```

Le e-mail automatiche per il programma di primo responder sono suddivise in due parti note come blocco introduzione e blocco richiesta dati.

Blocco di introduzione

Il blocco di introduzione è una stringa statica inclusa in ogni messaggio di posta elettronica del primo destinatario. Questa frase introduttiva serve semplicemente a fornire il contesto ai blocchi di richiesta dati. Di seguito è riportato un esempio di blocco di introduzione:

```
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:
```

Blocco richiesta dati

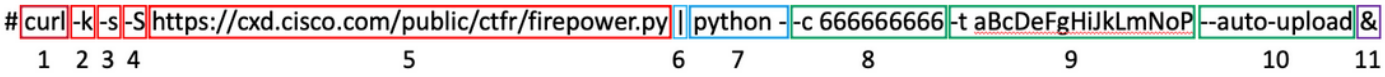
I blocchi di richiesta dati costituiscono il cuore del primo programma responder. Ogni blocco è costituito da una serie di passaggi predefiniti per la raccolta di dati per una determinata tecnologia. Come indicato nella sezione **Informazioni di base**, ogni blocco di richiesta di dati viene mappato a una tecnologia specifica. Questa è la stessa tecnologia scelta per aprire una richiesta di assistenza. In genere l'e-mail automatica contiene un singolo blocco di richiesta dati. Tuttavia, se alla tecnologia scelta è associato più di un blocco di richiesta dati, nel messaggio di posta elettronica vengono incluse più richieste di dati. Di seguito è riportato un esempio di formato del blocco Richiesta dati con più richieste di dati:

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

Ad esempio, nel caso di Secure Firewall, i blocchi di richiesta di dati multipli sono spesso inclusi quando viene inoltrata una richiesta di assistenza con problemi di VPN ad accesso remoto (RA-VPN) con Firepower Threat Defense (FTD), in quanto la tecnologia VPN ha anche un blocco di richiesta di dati mappato configurato per l'assistenza a raccogliere i bundle DART.

Comando generato

Nello specifico, per il caso di utilizzo Secure Firewall, come parte dell'e-mail automatizzata viene generato un unico comando di una riga per ogni caso. Di seguito è riportata una descrizione dettagliata della struttura del comando a riga singola:



1. Il comando curl viene utilizzato per scaricare l'ultima versione dello script firepower.py
2. Il flag **-k** consente a curl di ignorare gli errori del certificato durante la connessione.
3. Il flag **-s** è un'opzione per l'esecuzione della curva in modalità silenziosa. Questa opzione viene utilizzata per sopprimere l'output normale dell'arricciatura in quanto è rumorosa.
4. Il flag **-S** è un'opzione che consente di visualizzare gli errori relativi ai riccioli. Questa opzione viene utilizzata per forzare la visualizzazione degli errori di output da parte di curl anche con l'opzione silent abilitata.
5. URL in cui è ospitata la versione più recente dello script firepower.py. Questo percorso indica al comando curl di estrarre il corpo più recente dello script da eseguire.
6. Si tratta di una pipe di Linux, che passa l'output del comando curl (il contenuto di uno script python) a un'istruzione di esecuzione nel passaggio successivo.
7. A questo punto, il file binario Python sul dispositivo viene chiamato con un "-" aggiuntivo. Ciò indica a python che l'origine è presa da stdin (poiché il contenuto dello script è reindirizzato da curl).
8. Il flag **-c** è un argomento di input per lo script firepower.py, che indica il numero di richiesta in cui caricare i dati. Il valore 666666666 dopo questa opzione è il numero di esempio.
9. Il flag **-t** è un argomento di input per lo script firepower.py, che indica un token univoco (password) generato per questo caso particolare. Il valore aBcDeFgHiJkLmNoP dopo questa

opzione è il token di esempio per questo caso.

10. Il flag **—auto-upload** è un argomento speciale per lo script firepower.py, che indica lo script da eseguire in modalità di automazione. Per ulteriori informazioni su questo argomento, vedere la sezione specifica per lo script.
11. Il comando **&** indica all'utente di eseguire l'intero comando in background, consentendo all'utente di continuare a interagire con la propria shell durante l'esecuzione dello script.

Nota: Il flag -k è richiesto per tutte le versioni FMC precedenti alla 6.4 e per tutte le versioni FTD precedenti alla 6.7, poiché il certificato radice utilizzato da CXD non è stato considerato attendibile dai dispositivi Firepower fino alla versione 6.4 e FTD 6.7. Ciò impedisce la verifica del certificato.

Script Firepower.py

L'obiettivo principale dello script è quello di generare e caricare un pacchetto diagnostico dal dispositivo Secure Firewall, noto come "risoluzione dei problemi". Per generare questo file di risoluzione dei problemi, lo script firepower.py chiama semplicemente lo script sf_troubleshoot.pl incorporato responsabile della creazione del bundle. Questo è lo stesso script che viene chiamato quando generiamo una risoluzione dei problemi dalla GUI. Oltre al file di risoluzione dei problemi, lo script ha anche la capacità di raccogliere altri dati di diagnostica non inclusi nel pacchetto di risoluzione dei problemi. Al momento, gli unici dati aggiuntivi che possono essere raccolti sono i file di base, ma possono essere estesi in futuro se necessario. Lo script può essere eseguito in modalità "Automazione" o "Interattiva":

Automazione

Questa modalità viene attivata quando si utilizza l'opzione "—auto-upload" durante l'esecuzione dello script. Questa opzione disabilita i prompt interattivi, abilita la raccolta di file di base e carica automaticamente i dati nella richiesta. Il comando a riga singola generato dall'e-mail automatizzata include l'opzione "—auto-upload".

Interattivo

Questa è la modalità di esecuzione predefinita per lo script. In questa modalità l'utente riceve una richiesta di conferma per la raccolta di ulteriori dati diagnostici, ad esempio i file di base. Indipendentemente dalla modalità di esecuzione, l'output significativo viene stampato sullo schermo e registrato in un file di log per indicare l'avanzamento dell'esecuzione degli script. Lo script è ampiamente documentato tramite commenti sul codice in linea e può essere scaricato/rivisto dal sito https://cxd.cisco.com/public/ctfr/firepower.py.

Output previsto dello script

Di seguito è riportato un esempio di esecuzione riuscita dello script:

```
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!
```

Questo esempio di output include il caricamento di file core. Se nel dispositivo non sono presenti file di base, viene visualizzato un messaggio "No core files found. Skipping core file processing" viene invece presentato.

Problemi comuni

Di seguito sono riportati alcuni problemi comuni che è possibile riscontrare (in ordine di processo/esecuzione):

Protezione posta elettronica/riscrittura URL

Spesso si osserva che l'utente finale dispone di un certo livello di protezione della posta elettronica che consente di riscrivere l'URL. In questo modo viene alterato il comando a riga singola generato come parte della posta elettronica automatizzata. Ciò determina un errore di esecuzione poiché l'URL di pull dello script è stato riscritto e non è valido. Di seguito è riportato un esempio del comando previsto su una riga:

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

Procedura di risoluzione

Se l'URL nel comando contenuto nell'e-mail è diverso da "https://cxd.cisco.com/public/ctfr/firepower.py", è probabile che sia stato riscritto. Per risolvere il problema, sostituire l'URL prima di eseguire il comando.

Errore DNS

Questo errore curl viene spesso visualizzato quando il dispositivo non è in grado di risolvere l'URL per scaricare lo script:

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

Procedura di risoluzione

Per risolvere il problema, controllare le impostazioni DNS nel dispositivo per assicurarsi che sia in grado di risolvere correttamente l'URL per continuare.

Impossibile aprire/creare il file di registro

Una delle prime operazioni che lo script tenta di eseguire è la creazione (o l'apertura, se esiste già) di un file di log denominato **first-responder.log** nella directory di lavoro corrente. Se l'operazione non riesce, viene visualizzato un errore che indica un problema di autorizzazione semplice:

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

Nell'ambito di questa operazione, tutti gli altri errori vengono identificati e stampati sullo schermo nel seguente formato:

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



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

Procedura di risoluzione

Per correggere l'errore, eseguire lo script come utente amministrativo, ad esempio "admin" o "root".

Impossibile aprire/scrivere il file di notifica

Come parte dell'esecuzione dello script, nel sistema viene creato un file di 0 byte denominato "first_responder_notification". Il file viene quindi caricato nella richiesta come parte dell'automazione di questo programma. Questo file viene scritto nella directory "/var/common". Se l'utente che esegue lo script non dispone di autorizzazioni sufficienti per scrivere file in questa directory, lo script visualizza l'errore:

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

Procedura di risoluzione

Per correggere l'errore, eseguire lo script come utente amministrativo, ad esempio "admin" o "root".

> **Nota:** Se viene rilevato un errore non correlato alle autorizzazioni, viene visualizzato un errore catch-all "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". Il corpo completo dell'eccezione è disponibile nel file **first-responder.log**.

Impossibile bloccare il file sf_troubleshoot.pid

Per garantire l'esecuzione di un solo processo di generazione di risoluzione dei problemi alla volta,

lo script di generazione di risoluzione dei problemi tenta di bloccare il file /var/sf/run/sf_troubleshoot.pid prima di procedere. Se lo script non riesce a bloccare il file, viene visualizzato un errore:

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

Procedura di risoluzione

Nella maggior parte dei casi, questo errore indica che è già in corso un'attività di generazione per la risoluzione dei problemi separata. A volte questo è il risultato dell'esecuzione accidentale del comando a riga singola due volte di seguito. Per risolvere il problema, attendere il completamento del processo di generazione di risoluzione dei problemi corrente e riprovare più tardi.

> **Nota:** Se si verifica un errore all'interno dello script sf_troubleshoot.pl, questo errore viene visualizzato sullo schermo **"Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error".** Il corpo completo dell'eccezione è disponibile nel file **first-responder.log**.

Problemi di caricamento

Nello script è disponibile una funzione di caricamento comune responsabile del caricamento di tutti i file durante l'esecuzione degli script. Questa funzione è semplicemente un wrapper Python per eseguire un comando curl upload per inviare i file alla richiesta. Per questo motivo, gli eventuali errori rilevati durante l'esecuzione vengono restituiti come codice di errore curl. In caso di errore di caricamento, sullo schermo viene visualizzato questo errore:

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

Controllare il file **first-responder.log** per verificare l'errore completo. In genere, il file first-responder.log ha il seguente aspetto:

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

Procedura di risoluzione

In questo caso, l'url ha restituito uno stato di uscita di **6** che significa **" Impossibile risolvere l'host "**. Si tratta di un semplice errore DNS durante il tentativo di risolvere il nome host **cxd.cisco.com** . Consultare la documentazione dell'URL per decodificare eventuali stati di uscita sconosciuti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).