Risoluzione dei problemi relativi al blocco FTD degli URL IP privati a causa di un problema di analisi SI

Sommario

Problema

I dispositivi FTD hanno iniziato a bloccare il traffico interno di produzione quando l'host URL contiene un indirizzo IP privato dopo aver ricevuto gli aggiornamenti del feed di rete/URL di Security Intelligence da Talos.

Il traffico interessato include URL come http://10.54.1.7:8200/v1/sys/health e http://172.31.14.7:9100. Il traffico è stato classificato come "Indirizzi IP privati come host" e bloccato dalle policy di Security Intelligence relative a Talos con verdetti come "URL Block", "blacklist" e "si, force_block". Questo comportamento ha un impatto sulle comunicazioni interne dei servizi e sulle operazioni aziendali.

Quando si esaminano le tracce di supporto del sistema FTD, è stato osservato questo comportamento di blocco:

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

Ambiente

- Cisco FTD versione 7.6.4 (gestito da FMC)
- Feed di Security Intelligence abilitati con categorie URL dannosi

- Servizi di produzione interna che utilizzano indirizzi IP privati negli URL
- Il problema si è verificato dopo gli aggiornamenti dell'URL/feed di rete di Security Intelligence da Talos

Informazioni sui registri di traccia del supporto di sistema:

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- Nei registri di traccia di supporto del sistema, viene stampato il valore della categoria.
- Valore categoria: [1048627]
- La mappatura del valore di categoria e del file di feed SI corrispondente è disponibile in FTD all'indirizzo:

Posizione in FTD: /ngfw/var/sf/siurl_download/url.rules

Percorso nel file Tshot: /file-contents/var/sf/siurl_download/url.rules

<#root>

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$
```

cat url.rules

```
# security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
```

```
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID


si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

Come interpretare le righe precedenti:

- Al contenuto del file denominato "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" è stato assegnato un ID categoria: 1048627
- Per verificare la categoria effettiva, aprire il file utilizzando vi e qualsiasi strumento di modifica e il nome della categoria è in primo piano.

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %

cat -n  8c3e31be-ca41-43c8-87cb-82a35b0f5213| more


     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- Utilizzando il percorso logico corrispondente i file di feed di Security Intelligence possono essere tracciati e uno degli aspetti importanti della raccolta delle prove è il download manuale dei file di feed di Security Intelligence da FTD a un computer locale.
- I feed di Security Intelligence vengono aggiornati a intervalli regolari e durante l'aggiornamento dei feed non esistono registri delle modifiche nel FMC e nel FTD che indicano le modifiche apportate.
- Scaricando il feed di Security Intelligence, è possibile acquisire un'istantanea del feed in quel momento e fornirla successivamente al BU/TALOS.

Risoluzione

La risoluzione prevede l'aggiornamento dei feed di Security Intelligence e l'implementazione di una soluzione temporanea in attesa di una correzione permanente del software.

Passaggio 1: Aggiorna feed di Security Intelligence

Aggiornare i feed di Security Intelligence per ottenere il contenuto corretto dei feed da Talos:

Passare a Policy > Security Intelligence in FMC e attivare manualmente un aggiornamento feed oppure attendere il completamento del ciclo di aggiornamento automatico.

Passaggio 2: Implementa soluzione temporanea (se il problema persiste)

Se il problema persiste dopo l'aggiornamento del feed, aggiungere gli URL o i domini interessati all'elenco "Non bloccare" come soluzione temporanea:

Passare a Policy > Security Intelligence e aggiungere gli URL IP privati all'elenco "Non bloccare" nella scheda URL.

Passaggio 3: Riabilita categoria URL dannosa

Dopo aver confermato che l'aggiornamento dei feed risolve il problema, aggiungere nuovamente la categoria "URL dannoso" alla configurazione di Security Intelligence:

Passare a Policy > Security Intelligence e riattivare la categoria "URL dannoso" nell'elenco Blocca.

Passaggio 4: Rimozione delle voci della soluzione alternativa

Rimuovere l'URL o i domini interessati dall'elenco "Non bloccare" una volta che la correzione

permanente è stata confermata e funzionante.

Passaggio 5: Convalida

Verificare che le destinazioni degli URL IP privati non siano più bloccate da Security Intelligence verificando gli URL precedentemente interessati e monitorando gli eventi di connessione in FMC.

Causa

Il problema è stato causato da un problema di analisi nel contenuto dei feed di Security Intelligence che ha influito sul comportamento FTD. Nel feed dell'intelligence di sicurezza, erano presenti URL con lunghezza superiore a 2047 caratteri.

Quando una voce supera la lunghezza supportata, è possibile che il problema sia dovuto al fatto che è stata caricata in modo non corretto come voce dannosa separata, bloccando potenzialmente il traffico non correlato. Questo comportamento viene registrato in Cisco bug ID: CSCww11335. Il problema è stato risolto tramite modifiche correttive apportate dal team Talos al contenuto del feed, con una correzione software permanente pianificata per una versione successiva per aggiungere guide di protezione che impediscono il verificarsi di eventi futuri.

Contenuto correlato

- ID bug Cisco: CSCww1135
- Supporto tecnico Cisco e download

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).