Problemen oplossen met FTD-blokkering van privé-IP-URL's als gevolg van SI Parsing-probleem

Inhoud

uitgifte

FTD-apparaten zijn begonnen met het blokkeren van intern productieverkeer wanneer de URL-host een privé-IP-adres bevat na het ontvangen van Security Intelligence-URL- / netwerkfeed-updates van Talos.

Het getroffen verkeer bevat URL's zoals http://10.54.1.7:8200/v1/sys/health en http://172.31.14.7:9100. Het verkeer wordt gecategoriseerd als "Private IP-adressen als host" en geblokkeerd door Talos-gerelateerde Security Intelligence-beleid met uitspraken, waaronder "URL Block", "blacklist" en "si, force_block". Dit gedrag heeft invloed op interne communicatie en bedrijfsactiviteiten.

Bij het onderzoeken van de FTD-systeemondersteuningssporen werd dit blokkeringsgedrag waargenomen:

```
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
```

milieu

- Cisco FTD versie 7.6.4 (FMC Managed)
- Beveiligingsinlichtingenfeeds ingeschakeld met URL-categorieën voor kwaadwillenden

- Interne productieservices met behulp van privé-IP-adressen in URL's
- Probleem opgetreden na updates van URL/netwerkfeed voor Security Intelligence van Talos

Logboeken voor systeemondersteuning begrijpen:

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

- In de traceerlogboeken voor systeemondersteuning wordt de categoriewaarde afgedrukt.
- Rubriekwaarde: [1048627]
- Toewijzing van categoriewaarde en corresponderend SI-feedbestand is beschikbaar in FTD op locatie:

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

Locatie in Tshoot-bestand: /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
```

Hoe de vorige regel(s) te interpreteren:

- De inhoud in het bestand met de naam "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" is toegewezen, categorie-ID: 1048627
- Om te controleren wat de werkelijke categorie is, opent u het bestand met vi en een willekeurig bewerkingsprogramma en de naam van de categorie staat bovenaan.

<#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
```

- Met behulp van het logische pad kunnen de bijbehorende Security Intelligence-feedbestanden worden getraceerd en een van de belangrijke aspecten van het verzamelen van bewijsmateriaal is het handmatig downloaden van de Security Intelligence-feedbestanden van FTD naar een lokale machine.
- Security Intelligence-feeds worden regelmatig bijgewerkt en tijdens de feed-update bestaan er geen wijzigingslogboeken op FMC en FTD die aangeven wat de wijzigingen hebben aangebracht.
- Door de Security Intelligence-feed te downloaden, kunt u op dat moment een momentopname van de feed maken en deze kan later aan de BU / TALOS worden verstrekt.

resolutie

De oplossing bestaat uit het updaten van de Security Intelligence-feeds en het implementeren van een tijdelijke oplossing in afwachting van een permanente softwarefixatie.

Stap 1: Inlichtingenfeeds voor beveiliging bijwerken

Update de Security Intelligence-feeds om de gecorrigeerde feedinhoud van Talos te verkrijgen:

Navigeer naar Beleid > Beveiligingsinformatie in het VCC en activeer handmatig een feed-update of wacht tot de automatische updatecyclus is voltooid.

Stap 2: Tijdelijke oplossing implementeren (als het probleem blijft bestaan)

Als het probleem zich blijft voordoen na de update van de feed, voegt u de betreffende URL's of domeinen toe aan de lijst "Niet blokkeren" als tijdelijke tijdelijke tijdelijke oplossing:

Navigeer naar Beleid > Beveiligingsinformatie en voeg de privé-IP-URL's toe aan de lijst "Niet blokkeren" onder het tabblad URL.

Stap 3: URL Malicious Category opnieuw inschakelen

Nadat u hebt bevestigd dat de update van de feed het probleem heeft opgelost, voegt u de categorie "Kwaadaardige URL" opnieuw toe aan de configuratie van de beveiligingsinformatie:

Navigeer naar Beleid > Beveiligingsinformatie en schakel de categorie "Kwaadaardige URL" opnieuw in onder de Bloklijst.

Stap 4: Verwijder workaround-items

Verwijder de betreffende URL / domeinen uit de lijst "Niet blokkeren" zodra de permanente oplossing is bevestigd en werkt.

Stap 5: Validatie

Controleer of privé-IP-URL-bestemmingen niet langer worden geblokkeerd door Security Intelligence door de eerder getroffen URL's te testen en de verbindingsevenementen in FMC te bewaken.

Oorzaak

Het probleem werd veroorzaakt door een parseringsprobleem in de Security Intelligence-feeds met inhoud die van invloed was op het FTD-gedrag. In de Security intelligence feed waren er URL's met een lengte langer dan 2047 tekens.

Wanneer een item de ondersteunde lengte overschrijdt, kan een deel van dit probleem worden veroorzaakt doordat het onjuist is geladen als een afzonderlijk kwaadaardig item, waardoor mogelijk niet-gerelateerd verkeer wordt geblokkeerd. Dit gedrag wordt gevolgd onder Cisco bug ID: CSCww11335. Het probleem werd opgelost door corrigerende wijzigingen door het Talos-team aan de feed-inhoud, met een permanente softwarefixatie gepland voor een latere release om bewakingsrails toe te voegen die toekomstige voorvallen voorkomen.

Gerelateerde inhoud

- ID Cisco-bug: CSCww11335
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.