Fehlerbehebung: FTD blockiert private IP-URLs aufgrund eines SI-Analyseproblems

Inhalt

Problem

FTD-Geräte haben mit der Blockierung des produktionsinternen Datenverkehrs begonnen, nachdem der URL-Host eine private IP-Adresse erhalten hatte, nachdem sie URL-/Netzwerk-Feed-Updates der Sicherheitsintelligenz von Talos erhalten hatten.

Der betroffene Datenverkehr umfasst URLs wie http://10.54.1.7:8200/v1/sys/health und http://172.31.14.7:9100. Der Datenverkehr wird als "Private IP-Adressen als Host" kategorisiert und durch Talos-bezogene Sicherheitsrichtlinien mit Urteilen wie "URL-Block", "Blacklist" und "si, force_block" blockiert. Dieses Verhalten beeinträchtigt die interne Servicekommunikation und die Geschäftsabläufe.

Bei der Untersuchung der FTD-Systemunterstützungsspuren wurde dieses Blockierverhalten beobachtet:

```
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
```

Umwelt

- Cisco FTD Version 7.6.4 (FMC verwaltet)
- Sicherheitsinformations-Feeds mit aktivierten URL-Kategorien "Bösartig"
- Interne Produktionsdienste, die private IP-Adressen in URLs verwenden

- Problem nach Aktualisierung der Sicherheitsdaten-URL/des Netzwerk-Feeds von Talos

Grundlegendes zu den Trace-Protokollen der Systemunterstützung:

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

- In den Ablaufverfolgungsprotokollen der Systemunterstützung wird ein Kategoriewert ausgegeben.
- Kategoriewert: [1048627]
- Die Zuordnung des Kategoriewerts und der entsprechenden SI-Feed-Datei ist in FTD unter folgender Adresse verfügbar:

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

Speicherort in Tshot-Datei: /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
```

Wie die vorherige(n) Zeile(n) zu interpretieren:

- Dem Inhalt der Datei mit dem Namen "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" wurde eine Kategorie-ID zugewiesen: 1048627
- Um zu überprüfen, was die eigentliche Kategorie ist, öffnen Sie die Datei mit vi und einem beliebigen Editor-Tool, und der Name der Kategorie ist oben.

<#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
```

- Mithilfe des logischen Pfads können entsprechende Security Intelligence-Feed-Dateien verfolgt werden. Ein wichtiger Aspekt der Beweisaufnahme ist das manuelle Herunterladen der Security Intelligence-Feed-Dateien von FTD auf ein lokales System.
- Sicherheitsinformations-Feeds werden in regelmäßigen Abständen aktualisiert. Während der Feed-Aktualisierung existieren keine Änderungsprotokolle für FMC und FTD, aus denen hervorgeht, welche Änderungen vorgenommen wurden.
- Wenn Sie den Security Intelligence-Feed herunterladen, können Sie zu diesem Zeitpunkt einen Snapshot des Feeds erstellen, der der BU/TALOS später bereitgestellt werden kann.

Auflösung

Die Lösung beinhaltet die Aktualisierung der Sicherheitsinformations-Feeds und die Implementierung einer temporären Problemumgehung, während auf eine dauerhafte Behebung der Softwareprobleme gewartet wird.

Schritt 1: Sicherheitsinformations-Feeds aktualisieren

Aktualisieren Sie die Sicherheitsinformations-Feeds, um den korrigierten Feed-Inhalt von Talos abzurufen:

Navigieren Sie zu Policies > Security Intelligence im FMC, und lösen Sie manuell eine Aktualisierung aus, oder warten Sie, bis der automatische Aktualisierungszyklus abgeschlossen ist.

Phase 2: Implementieren der temporären Problemumgehung (wenn das Problem weiterhin besteht)

Wenn das Problem nach der Feed-Aktualisierung weiterhin besteht, fügen Sie die betroffenen URLs oder Domänen der Liste "Nicht blockieren" als temporäre Problemumgehung hinzu:

Navigieren Sie zu Policies > Security Intelligence (Richtlinien > Sicherheitsinformationen), und fügen Sie die privaten IP-URLs auf der Registerkarte URL der Liste "Nicht blockieren" hinzu.

Schritt 3: Neuaktivierung der schädlichen URL-Kategorie

Nachdem bestätigt wurde, dass das Problem durch die Feed-Aktualisierung behoben wurde, fügen Sie die Kategorie "URL Malicious" (URL schädlich) erneut zur Security Intelligence-Konfiguration hinzu:

Navigieren Sie zu Richtlinien > Sicherheitsinformationen, und aktivieren Sie die Kategorie "URL schädlich" in der Sperrliste erneut.

Schritt 4: Problemumgehungseinträge entfernen

Entfernen Sie die betroffenen URL/Domänen aus der Liste "Nicht blockieren", sobald der dauerhafte Fix bestätigt wurde und funktioniert.

Schritt 5: Validierung

Vergewissern Sie sich, dass private IP-URL-Ziele nicht mehr von der Sicherheitsintelligenz blockiert werden, indem Sie die zuvor betroffenen URLs testen und die Verbindungsereignisse im FMC überwachen.

Ursache

Das Problem wurde durch ein Analyseproblem in den Sicherheitsinformations-Feeds verursacht, das sich auf das FTD-Verhalten auswirkte. Der Sicherheitsinformations-Feed enthielt URLs mit einer Länge von mehr als 2047 Zeichen.

Wenn ein Eintrag die unterstützte Länge überschreitet, kann ein Teil dieses Problems darin liegen, dass er fälschlicherweise als separater bösartiger Eintrag geladen wurde, der möglicherweise nicht damit zusammenhängenden Datenverkehr blockiert. Dieses Verhalten wird unter der Bug-ID von Cisco verfolgt: CSCww11335. Das Problem wurde durch korrigierende Änderungen des Talos-Teams am Feed-Inhalt behoben. Für eine spätere Version war ein permanenter Software-Fix geplant, um Schutzschienen hinzuzufügen und zukünftige Ereignisse zu verhindern.

Verwandte Inhalte

- Cisco Bug-ID: CSW11335
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.