Resolución de problemas de bloqueo de FTD de URL de IP privadas debido a un problema de análisis de SI

Contenido

Problema

Los dispositivos FTD comenzaron a bloquear el tráfico interno de producción cuando el host URL contiene una dirección IP privada después de recibir actualizaciones de fuentes de red/URL de inteligencia de seguridad de Talos.

El tráfico afectado incluye URL como http://10.54.1.7:8200/v1/sys/health y http://172.31.14.7:9100. El tráfico se está categorizando como "Direcciones IP privadas como host" y se está bloqueando por las políticas de inteligencia de seguridad relacionadas con Talos con veredictos que incluyen "Bloqueo de URL", "lista negra" y "si, force_block". Este comportamiento afecta a las comunicaciones de servicios internos y a las operaciones empresariales.

Al examinar los seguimientos de compatibilidad del sistema FTD, se observó este comportamiento de bloqueo:

```
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
```

Entorno

- Cisco FTD versión 7.6.4 (gestionado por FMC)
- Fuentes de inteligencia de seguridad habilitadas con categorías malintencionadas de URL

- Servicios de producción internos que utilizan direcciones IP privadas en direcciones URL
- Problema tras las actualizaciones de la fuente de red/URL de inteligencia de seguridad de Talos

Introducción a los registros de seguimiento de compatibilidad del sistema:

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

- En los registros de seguimiento de compatibilidad del sistema, se imprime el valor de categoría.
- Valor de categoría: [1048627]
- La asignación del valor de categoría y el archivo de alimentación de SI correspondiente está disponible en FTD en la ubicación:

Ubicación en FTD: /ngfw/var/sf/siurl_download/url.rules

Ubicación en el archivo Tshoot: /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
```

Cómo interpretar las líneas anteriores:

- Al contenido del archivo con el nombre "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" se le ha asignado la ID de categoría: 1048627
- Para comprobar cuál es la categoría real, abra el archivo con vi y cualquier herramienta de edición, y el nombre de la categoría aparecerá en la parte superior.

<#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
```

- Se puede rastrear el uso de la ruta lógica correspondiente a los archivos de fuente de inteligencia de seguridad, y uno de los aspectos importantes de la recopilación de pruebas es descargar manualmente los archivos de fuente de inteligencia de seguridad de FTD a una máquina local.
- Las fuentes de inteligencia de seguridad se actualizan a intervalos regulares y, durante la actualización de la fuente, no existen registros de cambios en el FMC y el FTD que indiquen los cambios realizados.
- Al descargar la fuente de inteligencia de seguridad, puede tomar una instantánea de la fuente en ese momento y se puede proporcionar a la BU/TALOS más tarde.

Resolución

La resolución implica la actualización de las fuentes de inteligencia de seguridad y la implementación de una solución temporal mientras se espera una corrección de software permanente.

Paso 1: Actualizar fuentes de inteligencia de seguridad

Actualice las fuentes de Security Intelligence para obtener el contenido corregido de Talos:

Navegue hasta Políticas > Inteligencia de seguridad en el FMC y active manualmente una actualización de fuente, o espere a que el ciclo de actualización automática se complete.

Paso 2: Implementar una solución temporal (si el problema continúa)

Si el problema continúa después de la actualización de la fuente, agregue las URL o dominios afectados a la lista "No bloquear" como solución temporal:

Navegue hasta Políticas > Inteligencia de seguridad y agregue las URL de IP privadas a la lista "No bloquear" en la pestaña URL.

Paso 3: Volver a habilitar categoría malintencionada de URL

Después de confirmar que la actualización de la fuente resuelve el problema, vuelva a agregar la categoría "URL maliciosa" a la configuración de Security Intelligence:

Navegue hasta Políticas > Inteligencia de seguridad y vuelva a habilitar la categoría "URL maliciosa" en la Lista de bloqueo.

Paso 4: Eliminar entradas de solución alternativa

Elimine los dominios/URL afectados de la lista "No bloquear" una vez que se confirme y funcione la corrección permanente.

Paso 5: Validación

Verifique que Security Intelligence ya no esté bloqueando los destinos de URL de IP privada probando las URL afectadas anteriormente y supervisando los eventos de conexión en FMC.

Causa

El problema se debió a un problema de análisis en el contenido de las fuentes de inteligencia de seguridad que afectó al comportamiento de FTD. En la fuente de inteligencia de seguridad, había URL con una longitud superior a 2047 caracteres.

Cuando una entrada supera la longitud admitida, parte de este problema puede deberse a que se cargó incorrectamente como entrada malintencionada independiente, lo que podría bloquear el tráfico no relacionado. Este comportamiento se rastrea bajo el ID de bug de Cisco: CSCww11335. El problema se resolvió mediante cambios correctivos realizados por el equipo de Talos en el contenido de la fuente, con una corrección de software permanente planeada para una versión posterior para agregar barandillas de protección para evitar futuras ocurrencias.

Contenido relacionado

- ID de falla de funcionamiento de Cisco: CSCww11335
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).