Solucionar problemas de bloqueio de URLs IP Privados do FTD devido ao problema de análise do SI

Contents

Problema

Os dispositivos de FTD começaram a bloquear o tráfego interno de produção quando o host de URL contém um endereço IP privado após receber atualizações de URL/feed de rede do Talos com inteligência de segurança.

O tráfego afetado inclui URLs como http://10.54.1.7:8200/v1/sys/health e http://172.31.14.7:9100. O tráfego está sendo categorizado como "Endereços IP privados como host" e bloqueado por políticas de inteligência de segurança relacionadas ao Talos com vereditos que incluem "Bloqueio de URL", "lista negra" e "si, force_block". Esse comportamento afeta as comunicações de serviço interno e as operações comerciais.

Ao examinar os rastreamentos de suporte do sistema FTD, este comportamento de bloqueio foi observado:

```
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 Versão 7.6.4 (Gerenciado pelo FMC)
- Feeds de Inteligência de Segurança habilitados com categorias de URL Mal-intencionado

- Serviços de produção interna usando endereços IP privados em URLs
- Ocorreu um problema após as atualizações de URL/feed de rede do Security Intelligence do Talos

Entendendo os logs de rastreamento de suporte do sistema :

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

- Nos logs de rastreamento de suporte do sistema, o valor da categoria é impresso.
- Valor da categoria: [1048627]
- O mapeamento do valor da categoria e do arquivo de feed SI correspondente está disponível no FTD no local:

Localização no FTD: /ngfw/var/sf/siurl_download/url.rules

Local no arquivo 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
```

Como interpretar as linhas anteriores:

- O conteúdo do arquivo com o nome "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" recebeu a ID de categoria: 1048627
- Para verificar qual é a categoria real, abra o arquivo usando vi e qualquer ferramenta de edição, e o nome da categoria estará no topo.

<#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
```

- Utilizando o caminho lógico correspondente, os arquivos de feed de Inteligência de segurança podem ser rastreados, e um dos aspectos importantes da coleta de evidências é fazer o download manual dos arquivos de feed de Inteligência de segurança do FTD para uma máquina local.
- Os feeds do Security Intelligence são atualizados a intervalos regulares e, durante a atualização dos feeds, não existem registros de alterações no FMC e no FTD que indiquem as alterações efetuadas.
- Ao fazer o download do feed Security Intelligence, você pode tirar um instantâneo do feed nesse momento e fornecê-lo à BU/TALOS posteriormente.

Resolução

A resolução envolve a atualização dos feeds de inteligência de segurança e a implementação de uma solução temporária enquanto aguarda uma correção permanente do software.

Passo 1: Atualizar Feeds de Inteligência de Segurança

Atualize os feeds de Inteligência de segurança para obter o conteúdo de feed corrigido do Talos:

Navegue para Policies > Security Intelligence no FMC e acione manualmente uma atualização de feed ou aguarde a conclusão do ciclo de atualização automática.

Passo 2: Implementar uma solução temporária (se o problema persistir)

Se o problema continuar após a atualização do feed, adicione os URLs ou domínios afetados à lista "Não bloquear" como uma solução temporária:

Navegue até Policies > Security Intelligence e adicione os URLs IP privados à lista "Do not block" na guia URL.

Passo 3: Reabilitar categoria mal-intencionada de URL

Depois de confirmar que a atualização do feed resolve o problema, adicione novamente a categoria "URL malicioso" à configuração do Security Intelligence:

Navegue até Policies > Security Intelligence e reative a categoria "URL Malicious" na Block List.

Passo 4: Remover Entradas de Solução Alternativa

Remova os URL/domínios afetados da lista "Não bloquear" depois que a correção permanente for

confirmada e estiver funcionando.

Passo 5: Validação

Verifique se os destinos de URL de IP privado não estão mais sendo bloqueados pelo Security Intelligence testando os URLs afetados anteriormente e monitorando os eventos de conexão no FMC.

Causa

O problema foi causado por um problema de análise no conteúdo de feeds de Inteligência de Segurança que afetou o comportamento de FTD. No feed Inteligência de segurança, havia URLs com mais de 2047 caracteres.

Quando uma entrada excede o comprimento permitido, parte desse problema pode ter ocorrido porque ela foi carregada incorretamente como uma entrada mal-intencionada separada, bloqueando potencialmente o tráfego não relacionado. Este comportamento é rastreado sob a ID de bug da Cisco: CSCww11335. O problema foi resolvido por meio de alterações corretivas feitas pela equipe do Talos no conteúdo do feed, com uma correção permanente de software planejada para uma versão posterior para adicionar trilhos de proteção, evitando futuras ocorrências.

Conteúdo relacionado

- ID de bug da Cisco: CSCww11335
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.