

FTD de firewall seguro - Lista de bloqueio de áudio de telefone por zoom devido a VDB mais antigo

Contents

Problema

Os usuários experimentam problemas de áudio com chamadas de telefone com zoom onde as chamadas se conectam, mas o áudio está faltando. O FTD está descartando pacotes de mídia UDP de intervalos de IP de zoom, mostrando-os como bloqueados listados pelo Snort em capturas de pacotes e contadores de descarte ASP.

Os sintomas específicos incluíram:

- O firewall está executando o Cisco Vulnerability Database (VDB) versão 427 ou anterior.
- O firewall contém uma regra de acesso que deve permitir o tráfego de Zoom com base nas IDs de aplicativo padrão de Zoom/RTP fornecidas pelo banco de dados do Firepower. A regra deve permitir todas essas portas através das AppIDs de Zoom, de acordo com appid.cisco.com:
 - Zoom do usuário (6243): 80.443/tcp
 - Download de zoom (4628): 80.443/tcp
 - Carregamento de zoom (4627): 80.443/tcp
 - Reunião com zoom (4629): 80/TCP
 - Áudio RTP (2475): 5004/UDP
 - SIP (426): 5060/UDP
- No entanto, a saída do packet-tracer mostra que o tráfego é descartado pelo motivo da lista de bloqueio "Bloqueado ou incluído na lista de bloqueio pelo pré-processador do firewall".

<#root>

Phase: 17
Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns

Config:

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(vrfid:0)

input-status: up

input-line-status: up

output-interface: Outside(vrfid:0)

output-status: up

output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- As capturas de pacotes mostram quedas com o motivo: "Snort-blacklist" (em inglês).

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- Nas saídas de rastreamento de suporte do sistema, o tráfego é adiado durante a correspondência de regras devido à identificação pendente do aplicativo. No entanto, o tráfego está mal identificado e bloqueado. O endereço IP é um IP público Zoom que requer acesso de acordo com o artigo Zoom [Firewall de rede Zoom ou configurações de servidor proxy](#).

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- Os rastreamentos de suporte do sistema indicam "candidato a cliente RTP retornou mensagens de erro inválido (-11)" e "terceiros retornaram mensagens desconhecidas (0)" quando os IPs de Zoom tentam responder.

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- O comando FTD show asp drop mostra o rápido incremento de quedas de lista de bloqueio.

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

Ambiente

- Cisco Firepower FTD versão 7.7.11 gerenciado pelo FMC
- Vulnerability Database (VDB) versão 427 ou anterior
- Snort versão 3.3.5.100-66
- Tráfego que afeta principalmente as sub-redes IP de Zoom 170.114.0.0/16 e 206.247.0.0/16, mas pode incluir outros IPs de Zoom

Resolução

ID de bug Cisco CSCwu22106 Solução alternativa - Implementação de regra de pré-filtro

1: Crie uma regra de pré-filtro para o tráfego Zoom.

Navegue até Policies > Access Control > Prefilter e crie uma nova regra com esta configuração:

- Nome da regra: Zoom - Pré-filtro
- Ação: Fastpath
- Zona de Origem: INTERFACE DE ENTRADA
- Zona de destino: INTERFACE DE SAÍDA
- Endereço de origem: qualquer um
- Porta de origem: qualquer um
- endereço de destino: Os intervalos de IP de zoom (170.114.0.0/16, 206.247.0.0/16) e qualquer outro especificado nas [configurações de firewall de rede ou servidor proxy de zoom](#).
- Porta de Destino: UDP 10000-64000

2: Configuração de Regra de Controle de Acesso Alternativa

Se a filtragem prévia não for preferencial, modifique a regra de política de controle de acesso existente removendo os identificadores de aplicativo Zoom e usando IP explícito e correspondência de porta:

- Nome da regra: Permitir Zoom
- Ação: Permissão
- Zona de Origem: INTERFACE DE ENTRADA
- Zona de destino: INTERFACE DE SAÍDA
- Endereço de origem: qualquer um
- Porta de origem: qualquer um
- endereço de destino: Os intervalos de IP de zoom (170.114.0.0/16, 206.247.0.0/16) e qualquer outro especificado nas [configurações de firewall de rede ou servidor proxy de zoom](#).
- Porta de Destino: UDP / "Zoom-Phone-Ports" (intervalo 10000 64000)
- Registro: (opcional, para monitorar o tráfego permitido)

3: Implante as alterações de configuração nos dispositivos de FTD e verifique se a funcionalidade de áudio bidirecional foi restaurada.

- Monitore os contadores de descarte ASP para confirmar se a listagem de bloqueio foi interrompida:

```
device# show asp drop
```

- Verifique se as capturas de pacote têm tráfego bidirecional bem-sucedido:

```
device# show capture
```

4: O defeito no ID de bug da Cisco CSCwu22106 foi resolvido na versão 428 do Cisco Vulnerability Database (VDB). Os dispositivos Firepower devem executar as versões mais recentes do VDB para evitar o impacto desse defeito. Da mesma forma, o defeito relacionado do ID de bug da Cisco CSCwn80786 foi resolvido na versão 395 do VDB.

Causa

Um defeito nas assinaturas de identificação de aplicativos do Cisco Secure Firewall no Vulnerability Database (VDB) versão 427 faz com que o tráfego de mídia do Zoom Phone seja classificado incorretamente e subsequentemente bloqueado pelo mecanismo de inspeção Snort. Esse comportamento é rastreado sob o bug da Cisco ID CSCwu22106 e o bug relacionado ID da Cisco CSCwn80786, que documenta o tratamento incorreto de endereços IP de zoom e fluxos de mídia quando IDs de aplicativo são usadas.

Conteúdo relacionado

- [Aplicar zoom às configurações do firewall de rede ou do servidor proxy](#)
- [Práticas recomendadas para pré-filtragem de fastpath](#)

- [ID de bug Cisco CSCwu22106 - Ampliação incorreta de endereços IP manipulados no VDB 427](#)
- [ID de bug Cisco CSCwn80786 - O detector de aplicação de zoom não detecta redes para telefone de zoom](#)
- [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.