

Firewall seguro FTD - Zoom de teléfono Lista de bloqueo de audio Debido a VDB más antiguo

Contenido

Problema

Los usuarios experimentan problemas de audio con las llamadas del teléfono con zoom en las que se conectan las llamadas pero falta audio. El FTD está descartando paquetes de medios UDP de rangos de IP de zoom, mostrándolos como bloqueados enumerados por Snort en capturas de paquetes y contadores de descarte ASP.

Los síntomas específicos incluyeron:

- El firewall ejecuta Cisco Vulnerability Database (VDB) versión 427 o posterior.
- El firewall contiene una regla de acceso que debe permitir el tráfico de Zoom basado en los ID de aplicación de Zoom/RTP predeterminados proporcionados por la base de datos de Firepower. La regla debe permitir todos estos puertos a través de las ApplID de Zoom, según appid.cisco.com:
 - UserZoom (6243): 80 443/tcp
 - Descarga de zoom (4628): 80 443/tcp
 - Carga de zoom (4627): 80 443/tcp
 - Zoom Meeting (4629): 80/tcp
 - Audio RTP (2475): 5004/udp
 - SIP (426): 5060/udp
- Sin embargo, la salida del rastreador de paquetes muestra que el tráfico es descartado por la razón de la lista de bloqueo "Bloqueado o en la lista negra por el preprocesador del 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

- Las capturas de paquetes muestran caídas con motivo: "snort-blacklist".

<#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

- En las salidas de seguimiento de soporte del sistema, el tráfico se aplaza durante la coincidencia de reglas debido a la identificación de aplicación pendiente. Sin embargo, el tráfico está mal identificado y en la lista de bloqueo. La dirección IP es una IP pública de Zoom que requiere acceso según el artículo de Zoom [Zoom firewall de red o configuración del 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

- Los seguimientos de compatibilidad del sistema indican que el candidato del cliente RTP devolvió mensajes de error no válido (-11) y que terceros devolvió desconocido (0) cuando las IP de zoom intentan 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

- El comando FTD show asp drop muestra el incremento rápido de las caídas de la lista de bloqueo.

<#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

Entorno

- Cisco Firepower FTD versión 7.7.11 gestionado por FMC
- Vulnerability Database (VDB) versión 427 o posterior
- Snort versión 3.3.5.1100-66
- Tráfico que afecta principalmente a las subredes IP de zoom 170.114.0.0/16 y 206.247.0.0/16, pero puede incluir otras IP de zoom

Resolución

Solución alternativa Cisco bug ID CSCwu22106 - Prefilter Rule Implementation

1: Cree una regla de filtro previo para el tráfico de zoom.

Navegue hasta Políticas > Control de acceso > Prefiltro y cree una nueva regla con esta configuración:

- 'Nombre de la regla Zoom-Prefiltro
- Acción: Trayectoria rápida
- Zona de origen: Interfaz de Entrada
- Zona de destino: INTERFAZ DE SALIDA
- Dirección de la fuente: cualquiera
- Puerto de Origen: cualquiera
- dirección de destino: Rangos IP de zoom (170.114.0.0/16, 206.247.0.0/16) y cualquier otro valor especificado en [Zoom de firewall de red o en la configuración del servidor proxy](#).
- Puerto de Destino: UDP 10000-64000

2: Configuración de reglas de control de acceso alternativas

Si no se prefiere el prefiltro, modifique la regla de directiva de control de acceso existente quitando los identificadores de aplicación Zoom y utilizando la coincidencia explícita de IP y puertos:

- 'Nombre de la regla Permitir zoom
- Acción: Permiso
- Zona de origen: Interfaz de Entrada
- Zona de destino: INTERFAZ DE SALIDA
- Dirección de la fuente: cualquiera
- Puerto de Origen: cualquiera
- dirección de destino: Rangos IP de zoom (170.114.0.0/16, 206.247.0.0/16) y cualquier otro valor especificado en [Zoom de firewall de red o en la configuración del servidor proxy](#).
- Puerto de Destino: UDP / "Zoom-Phone-Ports" (intervalo 10000 64000)
- Registro: (opcional, para supervisar el tráfico permitido)

3: Implemente los cambios de configuración en los dispositivos FTD y verifique que se restaure la funcionalidad de audio bidireccional.

- Supervise los contadores de caídas de ASP para confirmar que se ha detenido la lista de bloqueo:

```
device# show asp drop
```

- Verifique las capturas de paquetes para el tráfico bidireccional exitoso:

```
device# show capture
```

4: El defecto ID de error de Cisco CSCwu22106 se resolvió en la versión 428 de la base de datos de vulnerabilidades de Cisco (VDB). Los dispositivos Firepower deben ejecutar las últimas versiones de VDB para evitar el impacto de este defecto. Del mismo modo, el defecto relacionado del ID de bug Cisco CSCwn80786 se resolvió en la versión 395 de VDB.

Causa

Un defecto en las firmas de identificación de la aplicación Cisco Secure Firewall en la versión 427 de la base de datos de vulnerabilidades (VDB) provoca que el tráfico de los medios del teléfono Zoom se clasifique erróneamente y, a continuación, se bloquee mediante el motor de inspección de Snort. Este comportamiento se rastrea bajo el Id. de bug Cisco CSCwu22106 y el defecto relacionado Id. de bug Cisco CSCwn80786, que documenta el manejo incorrecto de las direcciones IP de Zoom y los flujos de medios cuando se utilizan los ID de aplicación.

Contenido relacionado

- [Ampliar la configuración del servidor proxy o firewall de red](#)
- [Prácticas recomendadas para el prefiltrado de ruta rápida](#)

- [Id. de error de Cisco CSCwu22106 - Zoom de direcciones IP manejadas incorrectamente en VDB 427](#)
- [ID de error de Cisco CSCwn80786: el detector de aplicaciones de zoom no detecta redes para el teléfono de zoom](#)
- [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).