

FTD firewall protetto - Zoom Phone Audio Blocklist Due vecchi VDB

Sommario

Problema

Gli utenti riscontrano problemi audio con le chiamate Zoom Phone dove le chiamate si connettono ma manca l'audio. L'FTD sta eliminando i pacchetti multimediali UDP dagli intervalli Zoom IP, mostrandoli come bloccati elencati da Snort in packet capture e dai contatori di rilascio ASP.

Sintomi specifici inclusi:

- Sul firewall è in esecuzione Cisco Vulnerability Database (VDB) versione 427 o precedente.
- Il firewall contiene una regola di accesso che deve consentire il traffico Zoom in base agli ID predefiniti dell'applicazione Zoom/RTP forniti dal database Firepower. La regola deve consentire tutte queste porte tramite gli AppID Zoom, in base a [appid.cisco.com](https://www.cisco.com/appid):
 - UserZoom (6243): 80.443/TCP
 - Download zoom (4628): 80.443/TCP
 - Zoom Upload (4627): 80.443/TCP
 - Zoom riunione (4629): 80/tcp
 - Audio RTP (2475): 5004/udp
 - SIP (426): 5060/udp
- Tuttavia, l'output packet-tracer mostra che il traffico viene scartato a causa del motivo dell'elenco a blocchi "Bloccato o messo in blacklist dal preprocessore 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

- Le acquisizioni dei pacchetti mostrano le perdite con il 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

- Negli output di traccia del supporto di sistema, il traffico viene rinviato durante la corrispondenza delle regole a causa dell'identificazione dell'applicazione in sospeso. Tuttavia, il traffico viene identificato erroneamente e classificato come bloccato. L'indirizzo IP è un indirizzo IP pubblico Zoom che richiede l'accesso in base all'articolo Zoom [Zoom](#) del [firewall di rete o alle impostazioni del server 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

- Le tracce di supporto del sistema indicano che il candidato del client RTP ha restituito un messaggio di errore non valido (-11) e che terze parti hanno restituito messaggi sconosciuti (0) quando gli IP di zoom tentano di rispondere.

<#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

- Il comando FTD show asp drop mostra l'incremento rapido delle perdite dell'elenco di blocco.

<#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 versione 7.7.11 gestito da FMC
- VDB (Vulnerability Database) versione 427 o precedente
- Snort versione 3.3.5.100-66
- Il traffico che interessa principalmente le subnet Zoom IP 170.114.0.0/16 e 206.247.0.0/16, ma può includere altri IP Zoom

Risoluzione

Risoluzione dei problemi relativi all'ID bug Cisco CSCwu2106 - Implementazione della regola di prefiltro

1: Creare una regola di prefiltro per il traffico di zoom.

Passare a Criteri > Controllo di accesso > Prefiltro e creare una nuova regola con questa configurazione:

- Nome regola: Zoom-Prefiltro
- Azione: Percorso rapido
- Zona di origine: INTERFACCIA DI INPUT
- Zona di destinazione: INTERFACCIA DI USCITA
- Source address: qualsiasi
- Porta di origine: qualsiasi
- Indirizzo di destinazione: Zoom intervalli IP (170.114.0.0/16, 206.247.0.0/16) e qualsiasi altro valore indicato in [Zoom firewall di rete o impostazioni del server proxy](#).
- Porta di destinazione: UDP 1000-6400

2: Configurazione alternativa delle regole di controllo di accesso

Se non si preferisce applicare il prefiltro, modificare la regola dei criteri di controllo di accesso esistente rimuovendo gli identificatori dell'applicazione Zoom e utilizzando la corrispondenza esplicita delle porte e degli indirizzi IP:

- Nome regola: Zoom - Consenti
- Azione: Allow (Autorizza)
- Zona di origine: INTERFACCIA DI INPUT
- Zona di destinazione: OUTPUT INTERFACE
- Source address: qualsiasi
- Porta di origine: qualsiasi
- Indirizzo di destinazione: Zoom intervalli IP (170.114.0.0/16, 206.247.0.0/16) e qualsiasi altro valore indicato in [Zoom firewall di rete o impostazioni del server proxy](#).
- Porta di destinazione: UDP / "Zoom-Phone-Ports" (intervallo 10000/64000)
- Registrazione: (facoltativo, per il monitoraggio del traffico consentito)

3: Distribuire le modifiche alla configurazione sui dispositivi FTD e verificare che la funzionalità audio bidirezionale sia ripristinata.

- Monitorare i contatori di rilascio ASP per verificare che l'elenco di blocco sia stato arrestato:

```
device# show asp drop
```

- Verificare le acquisizioni dei pacchetti per il traffico bidirezionale corretto:

```
device# show capture
```

4: Difetto L'ID bug Cisco CSCwu22106 è stato risolto nella versione 428 di Cisco Vulnerability Database (VDB). I dispositivi Firepower devono eseguire le versioni più recenti di VDB per evitare l'impatto di questo difetto. Analogamente, il problema correlato con l'ID bug Cisco CSCwn80786 è stato risolto nella versione VDB 395.

Causa

Un difetto nelle firme di identificazione dell'applicazione Cisco Secure Firewall nella versione 427 del database di vulnerabilità (VDB) causa una classificazione errata del traffico multimediale di Zoom Phone e il successivo blocco elencato dal motore di ispezione Snort. Questo comportamento viene registrato in Cisco bug ID CSCwu22106 e il relativo errore Cisco bug ID CSCwn80786, che documenta la gestione errata degli indirizzi IP dello zoom e dei flussi multimediali quando si usano gli ID delle applicazioni.

Contenuto correlato

- [Ingrandire le impostazioni del firewall di rete o del server proxy](#)
- [Procedure ottimali per il prefiltro fastpath](#)
- [Cisco bug ID CSCwu22106 - Zoom degli indirizzi IP non gestito correttamente in VDB 427](#)
- [Cisco ID bug CSCwn80786 - Il rilevatore dell'applicazione dello zoom non rileva le reti per il telefono dello zoom](#)

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).