

Secure Firewall FTD - Zoom Telefon Audio Blocklist Aufgrund älterer VDB

Inhalt

Problem

Bei Zoom-Telefonanrufen treten Audioprobleme auf, wenn Anrufe verbunden werden, aber kein Audio vorhanden ist. Die FTD verwirft UDP-Medienpakete aus Zoom-IP-Bereichen und zeigt an, dass sie von Snort in Paketerfassungen und ASP-Drop-Zählern blockiert werden.

Spezifische Symptome:

- Auf der Firewall wird die Cisco Vulnerability Database (VDB) Version 427 oder älter ausgeführt.
- Die Firewall enthält eine Zugriffsregel, die den Zoom-Datenverkehr anhand der standardmäßigen Zoom-/RTP-Anwendungs-IDs der FirePOWER-Datenbank erlauben muss. Die Regel muss alle diese Ports über die Zoom-App-IDs erlauben, so appid.cisco.com:
 - UserZoom (6243): 80.443/TCP
 - Zoom-Download (4628): 80.443/TCP
 - Zoom-Upload (4627): 80.443/TCP
 - Konferenz vergrößern (4629): 80/TCP
 - RTP-Audio (2475): 5004/udp
 - SIP (426): 5060/udp
- Die Paketverfolgungsausgabe zeigt jedoch an, dass der Datenverkehr aufgrund der Sperrliste "Vom Firewall-Präprozessor blockiert oder auf Blacklist gesetzt" fallen gelassen wird.

<#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

- Bei Paketerfassungen werden Verwerfungen mit folgendem Grund angezeigt: "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

- Bei Trace-Ausgaben der Systemunterstützung wird der Datenverkehr beim Regelabgleich aufgrund der ausstehenden Anwendungsidentifizierung zurückgestellt. Der Datenverkehr wird jedoch falsch identifiziert und blockiert. Die IP-Adresse ist eine öffentliche Zoom-IP, die den Zugriff gemäß dem Zoom-Artikel [Netzwerkfirewall oder Proxy-Servereinstellungen vergrößern](#) muss.

<#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

- Die Traces für die Systemunterstützung zeigen an, dass "RTP-Client-Kandidat gab Fehlerungültig zurück (-11)" und "Drittanbieter gab unbekannt zurück (0)" Meldungen, wenn Zoom-IPs versuchen zu reagieren.

<#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

- Der FTD-Befehl `show asp drop` zeigt die schnelle Inkrementierung von Sperrlisten-Drops an.

```
<#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

Umwelt

- Cisco Firepower FTD Version 7.7.11, verwaltet von FMC
- Vulnerability Database (VDB) Version 427 oder älter
- Snort, Version 3.3.5.1100-66
- Datenverkehr, der hauptsächlich die Zoom-IP-Subnetze 170.114.0.0/16 und 206.247.0.0/16 betrifft, kann aber auch andere Zoom-IPs umfassen

Auflösung

Cisco Bug-ID CSCwu22106 Workaround - Implementierung von Vorfilterregeln

1: Erstellen Sie eine Vorfilterregel für den Zoom-Datenverkehr.

Navigieren Sie zu Policies > Access Control > Prefilter, und erstellen Sie eine neue Regel mit der folgenden Konfiguration:

- Regelname: Zoom-Vorfilter
- Aktion: FastPath
- Quellzone: EINGABESCHNITTSTELLE
- Zielzone: AUSGANGSSCHNITTSTELLE
- Source address: Beliebig
- Quell-Port: Beliebig
- Zieladresse: Zoom-IP-Bereiche (170.114.0.0/16, 206.247.0.0/16) und alle anderen in [Zoom-Netzwerk-Firewall- oder Proxy-Servereinstellungen](#) angegebenen Bereiche.
- Ziel-Port: UDP 10000-64000

2: Konfiguration der alternativen Zugriffskontrollregel

Wenn keine Vorfilterung bevorzugt wird, ändern Sie die vorhandene Zugriffskontrollrichtlinie, indem Sie Anwendungskennungen für Zoom entfernen und explizite IP- und Portzuordnung verwenden:

- Regelname: Zoom zulassen
- Aktion: Zulassen
- Quellzone: EINGABESCHNITTSTELLE
- Zielzone: AUSGANGSSCHNITTSTELLE
- Source address: Beliebig
- Quell-Port: Beliebig
- Zieladresse: Zoom-IP-Bereiche (170.114.0.0/16, 206.247.0.0/16) und alle anderen in [Zoom-Netzwerk-Firewall- oder Proxy-Servereinstellungen](#) angegebenen Bereiche.
- Ziel-Port: UDP / "Zoom-Phone-Ports" (Bereich 10000 64000)
- Protokollieren: (optional zur Überwachung des zulässigen Datenverkehrs)

3: Stellen Sie die Konfigurationsänderungen auf den FTD-Geräten bereit, und vergewissern Sie sich, dass die bidirektionale Audiofunktion wiederhergestellt ist.

- Überwachen von ASP-Ablagerungszählern, um zu bestätigen, dass die Sperrliste angehalten wurde:

```
device# show asp drop
```

- Überprüfung der Paketerfassung auf erfolgreichen bidirektionalen Datenverkehr:

```
device# show capture
```

4: Der Fehler Cisco bug ID CSCwu22106 wurde in der Version 428 der Cisco Vulnerability Database (VDB) behoben. FirePOWER-Geräte müssen die neuesten VDB-Versionen ausführen, um die Auswirkungen dieses Fehlers zu vermeiden. Ebenso wurde der zugehörige Fehler Cisco bug ID CSCwn80786 in VDB Version 395 behoben.

Ursache

Ein Fehler in den Cisco Secure Firewall-Anwendungskennungssignaturen in der Vulnerability Database (VDB) Version 427 führt dazu, dass Zoom Phone-Mediendatenverkehr falsch klassifiziert und anschließend von der Snort Inspection Engine blockiert wird. Dieses Verhalten wird unter der Cisco Bug-ID CSCwu22106 und dem zugehörigen Defekt Cisco Bug-ID CSCwn80786 nachverfolgt, der die falsche Behandlung von Zoom-IP-Adressen und Medien-Flows bei Verwendung von Anwendungs-IDs dokumentiert.

Verwandte Inhalte

- [Vergrößerung der Einstellungen für Netzwerk-Firewall oder Proxy-Server](#)
- [Best Practices für die FastPath-Vorfilterung](#)
- [Cisco Bug-ID CSCwu22106 - IP-Adressen im Zoom falsch in VDB 427 behandelt](#)
- [Cisco Bug-ID CSCwn80786 - Die Zoom-Anwendungserkennung erkennt keine Netzwerke für das Zoom-Telefon.](#)

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.