

توصى ليجست رظح - FTD نمآلآ ةيماحل رادج VDB دوجول ارظن ؛ ريغصتال/ريبككتل فتاهل ميدق

تايوتحمل

ةلأسم

نكلو تاملكملا لصتت شيح Zoom Phone تاملكم عم ةيتوص تالكشم نومدختسملا هجاوي
ةروطحمك اهرهظي و Zoom IP تاقاطن نم UDP طئاسو مزح طاقساب FTD موقي .دوقم توصلا
ASP طاقساب تادادعو مزحل طاقتل تايلمع في Snort لبق نم

يولي ام يلع ةدحمل ضارعال تلمتشاو

- رادصا وأ 427 رادصاإ Cisco Vulnerability Database (VDB) ليغشتب ةيماحل رادج موقي
مدقا

- ريغصتال/ريبككتل رورم ةكرحب حمست نأ بجي لوصو ةدعاق يلع ةيماحل رادج يوتحي
ةدعاق اهرفوت يتل ةيضارتفال ريغصتال/ريبككتل قيبطت تافرم يلا اذانتسا
تافرم لالخن نم ذفانملا هذه ةفاكل ةدعاقال حمست نأ بجي .Firepower تانايب
appid.cisco.com اقفو ،ريغصتال/ريبككتل تاقيبطت

- 80.443/tcp (6243) مدختسملا ريغصتال/ريبككت

- 80.443/tcp (4628) ريغصتال/ريبككتل ليكنت

- 80.443/tcp (4627) ريبككتل ليمحت

- TCP/80 لوكتورب (4629) ريبككتل عامتجا

- 5004/UDP RTP (2475) توص

- 5060/UDP SIP (426 راي عم) لوكتورب

- ةمئاق ببس ةطساوب اهطاقسا متي رورملا ةكرح نأ Packet-tracer جارخا رهظي ،كلذ عم و
"قبسملا ةيماحل رادج جلاع م ةطساوب ءادوسلا ةمئاقلا في ةجر دم وأ ةروطحم" رظحلا

<#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, dst sgt

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 inspect

- "ءادوسل ريخشل ةمئاق": ببسل طوقسل تاي لمع مزحل طاقتل تاي لمع رهظت

<#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

- ببسل ةدعاقل ةقباطم ءانثأ رورمل ةكرح ليجأت متي ،م اظنل ا م عدد عبتت تاجرم في متوحي حص ريغ لكشب رورمل ةكرح فيرعت مت ،كلذ عمو .قل عمل قي بطتل فيرعت [راذج تاداعل](#) اقفل و لوصول بلطتي ريغصت لل/ري بكتلل IP ناونع وه IP ناونع .اهرظح ري بكتلل لاقمل [ليكول مداخل](#) و [ةكبشلا ةيامح](#)

<#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: 268434438,
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 = 268434
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, logFlag
206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110391
206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1 -> 3
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, Detection 0
206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1
Verdict: blacklist

• ريغ لئاسر عاجراب ماق RTP لئاسر حشرم" نأ إلى ماظننل معد بقعت تاي لمع ريشت
Zoom IP ةلواحم دنع "(0) ةفورعم ريغ لئاسر عاجراب ثلاثل فرطال ماق" و"(-11) ةححص
درلل.

<#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

- رطحال ةمئاق طاقسإ تالاح ي ف ةعيرس ةدايز FTD show asp drop رمأ ضرعي

<#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

ةئيبلا

- FMC لبق نم ةرادملا 7.7.11 رادصلإ، Cisco Firepower FTD
- مدقأ رادصلإ وأ 427 رادصلإ (VDB) تارغثلا تانايب ةدعاق
- snort 3.3.5.1100-66 رادصلإ
- و Zoom IP 170.114.0.0/16 ةيعرفلا تاكبشلا ىلع يساسأ لكشب رورملا ةكرح رثؤت ريغصتلا/ريبككتلل ىرخأ IP نيوانع نمضتت نأ نكمي نكلو، 206.247.0.0/16

رارق

ةدعاق ذي فنت - Cisco CSCwu22106 نم ءاطخألا حيحصت فرع مل ليدب لح
ةقبسمل ةيفصتلا

ريبيكتال رورم ةكرحل قبس م ةيفصت لماع ةدعاق عاشناب مق 1:

اذه مادختساب ةديج ةدعاق عاشناب Prefilter > لوصولا يف مكحتال > تاسايسلا ىلإ لقتنا نيوكتال:

- قبسمل ريبيكتال حشرم :ةدعاقال مسا
- عيرس راسم :عارجالا
- لاخدإلا ةهجاو :ردصملا ةقطنملا
- جارجالا ةهجاو :ةهجولا ةقطنم
- يأ :ردصملا ناووع
- يأ :ردصملا ذفنم
- ةروكذم ىرخأ تاقاطن يأو (170.114.0.0/16، 206.247.0.0/16) Zoom IP تاقاطن :ةهجولا ناووع
[لليكولامدخاللا وأ ةكبشلا ةيامح رادج تادادع](#)ا يف
- UDP 10000-64000 :ءانيم ةياغ

ليدبل لوصولا يف مكحتال ةدعاق نيوكت 2:

"لوصولاب مكحتال ةسايس" ةدعاق ليذعتب مقف ،ةلضفم ةقبسمل ةيفصتال نكت مل اذا ةقباطم و IP ةقباطم مادختساو ريغصتال/ريبيكتال قيبطت تافرعم ةلازا قيرط نع ةدوجوملا :حيرصلال ذفانملا

- ريغصتال/ريبيكتالاب حامسلا :ةدعاقال مسا
- حامس :عارجالا
- لاخدإلا ةهجاو :ردصملا ةقطنملا
- OUPUT ةهجاو :ةهجولا ةقطنم
- يأ :ردصملا ناووع
- يأ :ردصملا ذفنم
- ةروكذم ىرخأ تاقاطن يأو (170.114.0.0/16، 206.247.0.0/16) Zoom IP تاقاطن :ةهجولا ناووع
[لليكولامدخاللا وأ ةكبشلا ةيامح رادج تادادع](#)ا يف
- (10000 64000 قاطنلا) "فتاهل/ريبيكتال ذفانم" / UDP :ءانيم ةياغ
- (اهب حومسمل رورملا ةكرح ةبقارمل ،يرايتخا) :ليجستال

يئاتنث توصلال فئاظو ةداعتسا نم ققحتو FTD ةزهجأ ىلع نيوكتلل تارييغت رشن ب مق: 3
هاتإلا

- جاردإلا رطح ديكأتل ةبقارم لل ASP طاقسا تادادع فاقيا مت

```
device# show asp drop
```

- ةحجانللا هاتإلا ةيئاتنثلا رورملا ةكرحل مزحلل طاقتلل نم ققحت

```
device# show capture
```

4: Cisco Vulnerability رادصا ي في Cisco CSCwu22106 نم ءاطخألا حيحصت فرعم ةلكشم لح مت: 4
VDB تارادصا ثدحأ ليغشتب FirePOWER ةزهجأ موقت نا بجي. 428 رادصاإلا (VDB Database)
نم ءاطخألا حيحصت فرعمب ةلصلال يذأطخألا لح مت، لثملابو. بيلعلا اذه نم ريثأتلل بنجل
VDB. نم 395 رادصاإلا ي في Cisco CSCwn80786

ببسلا

Cisco نم نمآلا ةيماحلل رادج قيبطت فيرعت تاعي قوت ي في ةدوجومللا بويعلال دحأ ببستي
طئاسو رورم ةكرح فينصت ي في (VDB) تارغلل تانايب ةدعاق نم 427 رادصاإلا لخاد ةدوجومللا
Snort. صرحف كرحم ةطساوب كلذ دعب اهرطح متو حيحصت ريغ لكشب فتاهللا ريغصت/ريبكت
تاذا بويعلالو Cisco CSCwu22106 نم ءاطخألا حيحصت فرعم تحت كولسللا اذه بقعت متي
ةحيحصت ريغ ةجلع قثوي يذالو، Cisco CSCwn80786 نم ءاطخألا حيحصت فرعمب ةلصلال
تاقيبطتلل تافرعم مادختسا دنع طئاسوللا تاقفدتو Zoom IP نيوانعل

ةلصلال يذو تحملا

- [ليكولل مداخل وأ ةكبشلا ةيماحل رادج تادادع ريغصت/ريبكت](#)
- [عيرسللا راسملل ةقبسمللا ةيفصتلل تاسراممللا لصفأ](#)
- [تمت يتللا IP نيوانع ريبكتب مق - Cisco CSCwu22106 نم ءاطخألا حيحصت فرعم](#)

VDB 427 ي ف حي حص ري غ ل كش ب اه ت ج ل اع م

- ق ي ب ط ت ف ش ت ك م ف ش ت ك ي ال - Cisco CSCwn80786 ن م ع ا ط خ أ ل ا ح ي ح ص ت ف ر ع م
ري غ ص ت ل ل ا / ر ي ب ك ت ل ا ف ت ا ه ت ا ك ب ش ر ي غ ص ت ل ل ا / ر ي ب ك ت ل ا
- Cisco ن م ت ا ل ي ز ن ت ل ا و ي ن ف ل ا م ع د ل ا

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا