Identificatie en beperking van exploitatie van de kwetsbaarheden van meerdere Cisco Unified Communications Manager en Presence Server

Identificatie en beperking van exploitatie van de kwetsbaarheden van meerdere Cisco Unified Communications Manager en Presence Server

Advies-ID: cisco-amb-20070711-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070711-cucm

Revisie 1.0

2007 juli 11 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document aan de volgende PSIRT Security Advisories: *Cisco Unified Communications Manager Overflow Vulnerabilities* en *Cisco Unified Communications Manager en Presence Server onbevoegde toegangskwetsbaarheden* en biedt identificatie- en onderdrukkingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in Cisco Unified Communications Manager en Cisco Unified Presence Server. Deze kwetsbaarheden worden in de volgende subsecties samengevat:

Overflow van de dienst van de Vertrouwen van het certificaat: Deze kwetsbaarheid kan op afstand zonder authentificatie en zonder gebruikersinteractie worden geëxploiteerd. Succesvolle benutting van deze kwetsbaarheid kan willekeurige codeuitvoering toestaan of een ontkenning van de dienst

(Dos) voorwaarde veroorzaken. De aanvalsvector is pakketten die worden verzonden naar de CTL-servicepoort (Certificate Trust List). De standaardpoort is TCP-poort 2444. Beheerders kunnen de poort die wordt gebruikt door de CTL-provider controleren door de Cisco Unified Communications Manager GUI te raadplegen: Kies **Systeem > Serviceparameters**. Kies de server in de vervolgkeuzelijst Server. Kies vervolgens **Cisco CTL Provider (Inactief)** of **Cisco CTL Provider (Actief)** uit de vervolgkeuzelijst Service. De term *(Inactief)* of *(Actief)* die aan de servicenaam in deze lijst is toegevoegd, geeft aan of de service is ingeschakeld. Nadat de service is geselecteerd, is de parameter Port Number zichtbaar in het gebied onder de vervolgkeuzelijsten Server en Service. De waarde voor deze parameter geeft de poort aan die wordt gebruikt voor de service wanneer deze actief is. Ten tijde van de publicatie was er geen CVE ID geassocieerd met deze kwetsbaarheid.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Realtime Information Server Data Collector Heap Overflow: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder authenticatie en zonder gebruikersinteractie. Succesvolle benutting van deze kwetsbaarheid kan willekeurige codeuitvoering toestaan of een ontkenning van de dienst (Dos) voorwaarde veroorzaken. De aanvalsvector is pakketten die naar de Real-Time Information Server (RIS) Data Collector poort worden verzonden. De standaardpoort is TCP-poort 2556. Beheerders kunnen de poort die wordt gebruikt door de RIS Data Collector-service controleren door de Cisco Unified Communications Manager GUI te raadplegen: Kies **Systeem > Serviceparameters**. Kies de server in de vervolgkeuzelijst Server. Kies vervolgens **Cisco RIS Data Collector (Inactief)** of **Cisco RIS Data Collector (Actief)** uit de vervolgkeuzelijst Service. De term *(Inactief)* of *(Actief)* die aan de servicenaam in deze lijst is toegevoegd, geeft aan of de service is ingeschakeld. Nadat de dienst is gekozen, is de RIS Cluster TCP-poortparameter zichtbaar in het gebied Clusterwide Parameters. De waarde voor deze parameter geeft de poort aan die wordt gebruikt voor de service wanneer deze actief is. Ten tijde van de publicatie was er geen CVE ID geassocieerd met deze kwetsbaarheid.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Onbevoegde beheerder kan Cisco Unified Communications Manager/Cisco Unified Presence Server System Services activeren/beëindigen: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder gebruikersinteractie. Bij een succesvolle exploitatie kan een ongeautoriseerde Cisco Unified Communications Manager/Cisco Unified Presence Server-beheerder systeemservices in een clusteromgeving activeren of beëindigen. Hierdoor kunnen kritische spraakdiensten worden onderbroken of stopgezet. De aanvalsvector is het SSL protocol dat TCP poort 8443 pakketten gebruikt. Zie Cisco CallManager TCP- en UDP-poortgebruik voor aanvullende informatie over de poorten die door de betreffende software worden gebruikt. Ten tijde van de publicatie was er geen CVE ID geassocieerd met deze kwetsbaarheid.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Onbevoegde beheerder kan SNMP-instellingen voor Cisco Unified Communications Manager/Cisco Unified Presence Server weergeven: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder gebruikersinteractie. Bij een succesvolle exploitatie kan een niet-geautoriseerde beheerder door de weergave SNMP-instellingen bladeren op de

beheerinterface van een Cisco Unified Communications Manager/Cisco Unified Presence Server-clusterknooppunt. De aanvalsvector is het SSL protocol dat TCP poort 8443 pakketten gebruikt. Zie Cisco CallManager TCP- en UDP-poortgebruik voor aanvullende informatie over de poorten die door de betreffende software worden gebruikt. Ten tijde van de publicatie was er geen CVE ID geassocieerd met deze kwetsbaarheid.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor de kwetsbaarheden die in dit document worden beschreven. Beheerders wordt aangeraden om veel van deze beveiligingsmethoden te beschouwen als algemene best practices op het gebied van beveiliging van infrastructuurapparaten en het verkeer dat het netwerk doorkruist.

Cisco IOS-software kan effectieve middelen voor explosiepreventie bieden door gebruik te maken van transittoegangscontrolelijsten (tACL's).

Effectieve explosiepreventie kan ook worden geboden door Cisco ASA 5500 Series adaptieve security applicatie, Cisco PIX 500 Series security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers die gebruikmaken van doorvoertoegangscontrolelijsten (tACL's).

Deze beveiligingsmechanismen filteren en neerzetten pakketten die proberen de in dit document beschreven kwetsbaarheden te exploiteren.

Cisco IOS NetFlow kan zichtbaarheid in exploitatiepogingen bieden door gebruik te maken van flowrecords. Cisco IOS-software, Cisco ASA, Cisco PIX-security applicaties en FWSM-firewalls kunnen zichtbaarheid bieden door syslogberichten en de tegenwaarden die worden weergegeven in de uitvoer van **show-**opdrachten.

Risicobeheer

Organisaties moeten hun standaardproces voor risicobeoordeling en risicobeperking volgen om de mogelijke gevolgen van deze kwetsbaarheden te bepalen. Triage verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk het meest succesvol zullen zijn. Cisco heeft documenten geleverd die organisaties kunnen helpen bij de ontwikkeling van een op risico gebaseerde triagecapaciteit voor hun informatieveiligheidsteams. Risico Triage voor Security Vulnerability Mededelingen en Risico Triage en Prototyping in Informatiebeveiliging Engagements kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

Waarschuwing: de effectiviteit van elke mitigatietechniek is afhankelijk van specifieke klantsituaties zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Voor deze hulpmiddelen is specifieke informatie over beperking en identificatie beschikbaar:

- Cisco IOS-routers en -Switches
- Cisco IOS NetFlow
- Cisco ASA-, PIX- en FWSM-firewalls

Cisco IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor douanevervoer

In een poging om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten, die internetverbindingspunten, partner- en leverancieraansluitpunten of VPN-verbindingspunten kunnen omvatten, moeten beheerders transittoegangscontrolelijsten (tACL's) implementeren om beleidshandhaving uit te voeren. Beheerders kunnen een tACL construeren door alleen geautoriseerd verkeer expliciet toe te staan om het netwerk op access points binnen te gaan of door geautoriseerd verkeer toe te staan om door het netwerk te reizen in overeenstemming met bestaand beveiligingsbeleid en configuraties.

Het tACL-beleid ontkent niet-geautoriseerde pakketten voor de CTL Provider-service op TCP-poort 2444, de RIS Data Collector op TCP-poort 2556 en de Cisco Unified Communications Manager/Cisco Unified Presence Server System Services op TCP-poort 8443 verzonden naar getroffen apparaten. In het volgende voorbeeld, 192.168.1.0/24 is de netwerkIP adresruimte die door de beïnvloede apparaten wordt gebruikt en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

Aanvullende informatie over ACL's is beschikbaar in Transit Access Control Lists: Filtering at Your Edge.

```
!-- Include any explicit permit statements for trusted sources !-- that require
access on the vulnerable port(s) ! access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2444 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2556 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 8443 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! access-list 150
deny tcp any 192.168.1.0 0.0.0.255 eq 2444 access-list 150 deny tcp any 192.168.1.0
0.0.0.255 eq 2556 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 ! !--
Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list 150 deny ip any any ! !-- Apply tACL to interface(s) in the ingress
direction interface GigabitEthernet0/0 ip access-group 150 in !
```

Merk op dat het filtreren met een lijst van de interfacetoegang de transmissie van onbereikbare berichten ICMP terug naar de bron van het gefilterde verkeer zal veroorzaken. Dit kan het ongewenste effect hebben van het verhogen van CPU-gebruik omdat het apparaat deze ICMP onbereikbare berichten moet genereren. In Cisco IOS-software is de onbereikbare ICMP-generatie standaard beperkt tot één pakket per 500 milliseconden. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met de opdracht interfaceconfiguratie **op ICMP onbereikbaar**. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met behulp van de **algemene** opdracht voor configuratie **ip icmp-snelheidslimiet voor onbereikbare** *interval-in-ms*.

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat de beheerder de tACL op een interface heeft toegepast, zal de opdracht **IP-toegangslijsten tonen** het aantal CTL-dienstpakketten voor providers identificeren op TCP-poorten 2444, RIS Data Collector-pakketten op TCP-poort 2556 en CUCM/CUPS System Service-pakketten op TCP-poort 8443 die zijn gefilterd. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten 150** volgt:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444 (2 matches)
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556 (3 matches)
    30 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443 (3 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 2444 (3 matches)
    50 deny tcp any 192.168.1.0 0.0.0.255 eq 2556 (4 matches)
    60 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 (5 matches)
    70 deny ip any any
router#
```

In het voorafgaande voorbeeld, toegangslijst 150 heeft **3 pakketten op TCP-poort 2444** laten vallen voor ACE-sequentie ID 40, **4 pakketten op TCP-poort 2556** voor ACE-sequentie ID 50, en **5 pakketten op TCP-poort 8443** voor ACE-sequentie ID 60.

Identificatie: Vastlegging toegangslijst

De optie **log-** of **log-input** ACL zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden vastgelegd. De **log-**inputoptie maakt het registreren van de toegangsinterface mogelijk, naast de IP-adressen en -poorten van de pakketbron en de bestemming.

Waarschuwing: vastlegging in toegangscontrolelijst kan zeer CPU-intensief zijn en moet met uiterste voorzichtigheid worden gebruikt. De CPU-impact van ACL-vastlegging wordt bepaald door twee factoren: processwitching als resultaat van pakketten die log-enabled ACE's en loggeneratie en transmissie matchen.

De CPU-impact van ACL-vastlegging kan worden aangepakt in hardware op de Catalyst 6500 Series-switches en Cisco 7600 Series-routers met Supervisor 720 en Supervisor 32 met behulp van geoptimaliseerde ACL-vastlegging. De opdracht **interval-***in-ms* **van de ip-toegangslijst**-vastlegging kan de effecten van processwitching beperken die worden geïnduceerd door ACL-vastlegging. De **logsnelheid-limiet** *rate-per-seconde* [**behalve** *loglevel*] opdracht beperkt het effect van loggeneratie en transmissie.

Voor extra informatie over de configuratie en het gebruik van ACL-vastlegging raadpleegt u het witboek Toegepaste Intelligentie op http://www.cisco.com/web/about/security/intelligence/acl-logging.html.

Cisco IOS NetFlow

Identificatie: Traffic Flow Identification met NetFlow-records

Beheerders kunnen Cisco IOS NetFlow configureren op Cisco IOS-routers en -switches om te helpen bij de identificatie van verkeersstromen die potentiële pogingen kunnen zijn om de kwetsbaarheden te exploiteren die in dit document worden beschreven. De beheerders zouden

stromen moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.201 Gi0/1         192.168.1.102   06 0984 098C     1
Gi0/0         192.168.100.5   Gi0/1         192.168.1.158   06 0911 09FC     3
Gi0/0         192.168.105.60  Gi0/1         192.89.1.226    06 0016 12CA     1
Gi0/0         192.168.105.97  Gi0/1         192.168.1.28    06 0B3E 098C     5
Gi0/0         192.168.105.197 Gi0/1         192.168.1.248   06 0B3E 20FB     7
Gi0/0         192.168.1.17    Gi0/1         192.168.1.97    11 0B89 00A1     1
Gi0/0         192.168.105.7   Gi0/1         192.168.1.8     06 0B3E 20FB     4
Gi0/1         10.88.226.1     Gi0/0         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.1.239   06 0E8A 09FC     1
Gi0/1         10.89.16.226    Gi0/0         192.168.150.60  06 12CA 0901     1
router#
```

In het bovenstaande voorbeeld zijn er verschillende stromen voor de CTL Provider-service op **TCP-poort 2444 (hex-waarde 098C)**, de RIS Data Collector op **TCP-poort 2556 (hex-waarde 09FC)** en de Cisco Unified Communications Manager/Cisco Unified Presence Server System Service op **TCP-poort 8443 (hex-waarde 20FB)**. Beheerders moeten deze stromen vergelijken met het gebruik van de basislijn voor verkeer dat op TCP-poorten 2444, 2556 en 8443 wordt verzonden en moeten ook de stromen onderzoeken om te bepalen of ze afkomstig zijn van niet-vertrouwde hosts of netwerken.

Als u alleen de verkeersstromen voor pakketten op TCP-poort 2444 (hex-waarde 098C), pakketten op TCP-poort 2556 (hex-waarde 09FC) of pakketten op TCP-poort 8443 (hex-waarde 20FB) wilt weergeven, **toont** de opdracht **ip-cachestroom | omvat SrcIf|_06_.*(098C|09FC|20FB)** de verwante verslagen NetFlow zoals hier getoond zal tonen:

```
router#show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.110  Gi0/1         192.168.1.163   06 0E2A 098C     6
Gi0/0         192.168.105.230  Gi0/1         192.168.1.20    06 0C09 098C     1
Gi0/0         192.168.101.131  Gi0/1         192.168.1.245   06 0B66 20FB    18
Gi0/0         192.168.100.7    Gi0/1         192.168.1.162   06 0D14 09FC     1
Gi0/0         192.168.100.86   Gi0/1         192.168.1.27    06 0B7B 09FC     2
router#
```

Cisco ASA-, PIX- en FWSM-firewalls

Beperking: toegangscontrolelijsten voor douanevervoer

In een poging om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten, die internetverbindingspunten, partner- en leverancieraansluitpunten of VPN-verbindingspunten kunnen omvatten, moeten beheerders tACL's implementeren om beleidshandhaving uit te voeren. Beheerders kunnen een tACL construeren door alleen geautoriseerd verkeer expliciet toe te staan om het netwerk op access points binnen te gaan of door geautoriseerd verkeer toe te staan om door het netwerk te reizen in overeenstemming met bestaand beveiligingsbeleid en configuraties.

Het tACL-beleid ontkent onbevoegde CTL-servicepakketten voor providers op TCP-poort 2444, RIS Data Collector-pakketten op TCP-poort 2556 en Cisco Unified Communications Manager/Cisco Unified Presence Server System-servicepakketten op TCP-poort 8443 verzonden naar getroffen apparaten. In het volgende voorbeeld, 192.168.1.0/24 is de netwerkIP adresruimte die door de beïnvloede apparaten wordt gebruikt en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

Aanvullende informatie over ACL's is beschikbaar in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include any explicit permit statements for trusted sources !-- that require
access on the vulnerable port(s) ! access-list Transit-ACL-Policy extended permit tcp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2556 access-list
Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq 8443 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
can aid in identification of attacks ! access-list Transit-ACL-Policy extended deny
tcp any 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy extended
deny tcp any 192.168.1.0 255.255.255.0 eq 2556 access-list Transit-ACL-Policy
extended deny tcp any 192.168.1.0 255.255.255.0 eq 8443 ! !-- Permit/deny all other
Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and
configurations ! !-- Explicit deny for all other IP traffic ! access-list Transit-
ACL-Policy extended deny ip any any ! !-- Apply tACL to interface(s) in the ingress
direction ! access-group Transit-ACL-Policy in interface outside !
```

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders de **show access-list** opdracht gebruiken om het aantal CTL Provider service pakketten te identificeren op TCP poort 2444, RIS Data Collector pakketten op TCP poort 2556, en Cisco Unified Communications Manager/Cisco Unified Presence Server System Service pakketten op TCP poort 8443 die zijn gefilterd. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont toegang-lijst Transit-ACL-Policy** volgt:

```
firewall# show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 7 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2444 (hitcnt=2) 0xaca1615c
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2556 (hitcnt=4) 0x991fbe7d
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 8443 (hitcnt=3) 0xd2687825
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2444 (hitcnt=19) 0xc81a715d
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2556 (hitcnt=11) 0x67db99e7
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.1.0255.255.255.0
            eq 8443 (hitcnt=7) 0xb322498f
access-list Transit-ACL-Policy line 7 extended deny ip any any(hitcnt=0) 0xc797eb99
firewall#
```

In het voorafgaande voorbeeld, heeft de toegangslijst Transit-ACL-Policy **19 pakketten voor TCP-poort 2444** laten vallen, **11 pakketten voor TCP-poort 2556**, en **7 pakketten voor TCP-poort 8443** ontvangen van een onbetrouwbare host of netwerk. Daarnaast kan syslog-bericht 106023 waardevolle informatie leveren, waaronder het IP-adres van de bron en de bestemming, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket.

Identificatie: berichten in Firewall Access List System

Het 106023 van het firewallsyslog zal voor pakketten worden geproduceerd die door ACE worden ontkend die niet het aanwezige **logboeksleutelwoord** heeft. Aanvullende informatie over dit syslogbericht is beschikbaar in het systeemlogbericht van Cisco Security Appliance - 106023.

Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie of de Cisco PIX 500 Series security applicatie is beschikbaar in Vastlegging configureren op de Cisco security applicatie. Informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series-switches en Cisco 7600 Series-routers is beschikbaar in Configureren van bewaking en vastlegging op Cisco FWSM.

In het volgende voorbeeld, de **show vastlegging | grep** *regexp* opdracht haalt syslog berichten uit de logboekbuffer op de firewall. Deze berichten verstrekken extra informatie over ontkende pakketten die op potentiële pogingen zouden kunnen wijzen om de kwetsbaarheden te exploiteren die in dit document worden beschreven. Het is mogelijk om verschillende reguliere expressies te gebruiken met het **grep**-sleutelwoord om te zoeken naar specifieke gegevens in de geregistreerde berichten.

Aanvullende informatie over de syntaxis van reguliere expressies is beschikbaar in Opdrachtlijninterface gebruiken.

```
firewall#show logging | grep 106023
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
            inside:192.168.1.191/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 dst
            inside:192.168.1.33/2556 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
            inside:192.168.1.240/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 dst
            inside:192.168.1.115/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
            inside:192.168.1.38/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 dst
            inside:192.168.1.250/2444 by access-group "Transit-ACL-Policy"
firewall#
```

In het vorige voorbeeld, tonen de berichten die voor het tACL Transit-ACL-Policy zijn geregistreerd pakketten voor **TCP-poort 2444**, pakketten voor **TCP-poort 2556**, en pakketten voor **TCP-poort 8443** die naar het adresblok zijn verzonden dat aan de netwerkinfrastructuur is toegewezen.

Er is aanvullende informatie over syslogberichten voor ASA- en PIX-beveiligingsapparaten beschikbaar in Cisco Security Appliance System Log Messages. Aanvullende informatie over syslog-berichten voor de FWSM is beschikbaar in Catalyst 6500 Series Switch en Cisco 7600 Series router Firewall Services Module Logging Configuration en System Log Berichten.

Aanvullende informatie

Revisiegeschiedenis

Revisie 1.0	2007-juli-11	Eerste openbare publicatie

Cisco-beveiligingsprocedures

Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dit omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op http://www.cisco.com/go/psirt.

Gerelateerde informatie

- Cisco-bulletins voor toegepaste beperking
- Uw kern beveiligen: toegangscontrolelijsten voor infrastructuurbescherming
- Transit Access Control Lists: filtering aan uw rand
- Vastlegging toegangscontrolelijst

- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- Cisco Firewallproducten - startpagina op Cisco.com
- Gemeenschappelijke kwetsbaarheids- en blootstellingslijst

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.