Identificatie en beperking van exploitatie van de kwetsbaarheden voor weigeringen van services in Cisco Unified Communications Manager en Cisco Intercompany Media Engine

Identificatie en beperking van exploitatie van de kwetsbaarheden voor weigeringen van services in Cisco Unified Communications Manager en Cisco Intercompany Media Engine

Advies-ID: cisco-amb-20110824-cucm-ime

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-ime

Revisie 1.1

Laatst bijgewerkt op 20 november 23:20 UTC (GMT)

2011 augustus 24 00:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document aan de PSIRT Security Advisories *Cisco Unified Communications Manager Denial of Service Vulnerabilities* en *Denial of Service Vulnerabilities in Cisco Intercompany Media Engine* en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in Cisco Unified Communications Manager en Intercompany Media Engine. De volgende subsecties vatten deze kwetsbaarheden samen:**DoS-kwetsbaarheid in Cisco Unified Communications Manager met enabled Packet Capture Service:** deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan het betreffende apparaat vastlopen. Herhaalde pogingen om

deze kwetsbaarheid te exploiteren kunnen resulteren in een aanhoudende ontkenning van de dienst (DoS) door het geheugen van de Unified Communications Manager uit te putten. De aanvalsvector voor exploitatie is via TCP-pakketten die een 3-weg TCP-handdruk naar de Unified Communications Manager voltooien en de verbindingen open laten.Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-2560.**DoS-kwetsbaarheid in Cisco Unified Communications Manager met bepaalde configuraties van MTP:** deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan het betreffende apparaat vastlopen. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie.De aanvalsvectoren voor exploitatie worden door pakketten gebruikt die de volgende protocollen en poorten gebruiken:

- Session Initiation Protocol (SIP) met TCP-poort 5060
- SIP over Transport Layer Security (TLS) met TCP-poort 5061
- SIP met UDP-poort 5060
- SIP met UDP-poort 5061

Een aanvaller kon deze kwetsbaarheden exploiteren met gespoofde pakketten.Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-2561.**DoS-kwetsbaarheid in Cisco Unified Communications Manager bij het verwerken van bepaalde SIP INVITE-berichten:** deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan het betreffende apparaat vastlopen. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie.De aanvalsvectoren voor exploitatie worden door pakketten gebruikt die de volgende protocollen en poorten gebruiken:

- SIP met TCP-poort 5060
- SIP-TLS over Transport Layer Security (TLS) met TCP-poort 5061
- SIP met UDP-poort 5060
- SIP-TLS met UDP-poort 5061

Een aanvaller kon deze kwetsbaarheden exploiteren met gespoofde pakketten.Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-2562.**Twee DoS-kwetsbaarheden in Cisco Unified Communications Manager en Cisco Intercompany Media Engine (IME) met Service Advertisement Framework (SAF):** deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan het betreffende apparaat vastlopen. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie.De aanvalsvectoren voor exploitatie worden gemaakt door:

- SAF-pakketten met TCP-poorten 5050 (voor Cisco Unified Communications Manager)
- SAF-pakketten met TCP-poort 5620 (voor IME)

Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2011-2563 en CVE-2011-2564.Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisories, die beschikbaar zijn op de volgende links: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-cucm en https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-ime.

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor deze kwetsbaarheden. Beheerders wordt aangeraden deze beveiligingsmethoden te beschouwen als algemene best practices op het gebied van beveiliging van infrastructuurapparaten en het verkeer dat het netwerk doorkruist. In dit gedeelte van het document wordt een overzicht van deze technieken gegeven.Cisco IOS-software kan effectieve middelen voor explosiepreventie bieden door gebruik te maken van de volgende methoden:

- Toegangscontrolelijsten voor douanevervoer (ACL's)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP-bronbeveiliging (IPSG)

Deze beschermingsmechanismen filteren en vallen, evenals verifiëren het bron IP adres van, pakketten die proberen om deze kwetsbaarheden te exploiteren.De juiste implementatie en configuratie van Unicast RPF biedt een effectieve bescherming tegen aanvallen die pakketten met IP-adressen van gespoofde bronnen gebruiken. Unicast RPF moet zo dicht mogelijk bij alle verkeersbronnen worden geïmplementeerd.De juiste plaatsing en configuratie van IPSG biedt een effectief middel tegen spoofingaanvallen op de toegangslaag.Omdat het potentieel bestaat dat een vertrouwde netwerkclient kan worden beïnvloed door een worm die geen pakketten met spoofed-bronadressen gebruikt, bieden Unicast RPF en IPSG geen volledige bescherming tegen deze kwetsbaarheden.De Cisco ASA 5500 Series adaptieve security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 kunnen ook zorgen voor effectieve middelen voor explosiepreventie.

- Toegangscontrolelijsten voor douanevervoer (ACL's)
- Unicast Reverse Path Forwarding (Unicast RPF)
- TCP-normalisatie

Deze beschermingsmechanismen filteren en vallen, evenals verifiëren het bron IP adres van, pakketten die proberen om deze kwetsbaarheden te exploiteren.Effectieve exploit-preventie kan ook worden geleverd door de Cisco ACE-applicatie en -module voor Application Control Engine met behulp van TCP-normalisatie.Dit beschermingsmechanisme filtert en laat pakketten vallen die proberen deze kwetsbaarheden te exploiteren.Effectief gebruik van de gebeurtenisacties van Cisco Inbraakpreventiesysteem (IPS) biedt zichtbaarheid in en bescherming tegen aanvallen die proberen deze kwetsbaarheden te exploiteren.Cisco IOS NetFlow-records kunnen zichtbaarheid bieden in netwerkgebaseerde exploitatiepogingen.Cisco IOS-software, Cisco ASA, FWSM-firewalls en Cisco ACE Application Control Engine-applicatie en -module kunnen zichtbaarheid bieden door middel van syslogberichten en tegenwaarden die worden weergegeven in de uitvoer van **show-**opdrachten.Het Cisco Security Monitoring, Analysis, and

Response System (Cisco Security MARS) applicatie kan ook zichtbaarheid bieden via incidenten, vragen en gebeurtenisrapportage.

Risicobeheer

Organisaties wordt aangeraden om hun standaardprocessen voor risico-evaluatie en -beperking te volgen om de potentiële impact van [deze kwetsbaarheid|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 aankondigingen en Risk Triage en Prototyping kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

Waarschuwing: de effectiviteit van elke mitigatietechniek hangt af 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- en FWSM-firewalls
- Cisco ACE
- Cisco-inbraakpreventiesysteem
- Cisco-systeem voor beveiligingsbewaking, analyse en respons

Cisco IOS-routers en -Switches**Beperking: toegangscontrolelijsten voor douanevervoer**Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten, die internetverbindingspunten, partner- en leverancierspunten of VPN-verbindingspunten kunnen omvatten, wordt beheerders aangeraden om transittoegangscontrolelijsten (tACL's) te 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. Een tACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheden bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.Het tACL-beleid ontkent onbevoegde SIP-, SAF- en SIP-TLS-pakketten op TCP- en UDP-poorten 5060 en 5061 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 en 2001:DB8:1:60:/64 zijn de IPv4 en IPv6 adresruimte, respectievelijk, die wordt gebruikt door de getroffen apparaten, en de host op 192.168.100.1 (2001:DB8:1:100::1 voor IPv6) wordt beschouwd als een vertrouwde bron die toegang tot de getroffen 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 tACL's staat in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require
access on the vulnerable protocols and ports ! access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit udp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit udp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050 access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list 150 deny deny tcp any 192.168.60.0
0.0.0.255 eq 5060 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq
5061 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-
list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150
deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 access-list 150 deny deny
tcp any 192.168.60.0 0.0.0.255 eq 5620 ! !-- Permit or 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 ! !-- Create the corresponding IPv6 tACL ! ipv6 access-list
IPv6-Infrastructure-ACL-Policy ! !-- Include explicit permit statements for
trusted sources !-- that require access on the vulnerable protocols and ports
! permit tcp host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit tcp
host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5050 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks to global and !-- link local addresses ! deny tcp
any 2001:DB8:1:60::/64 eq 5060 deny tcp any 2001:DB8:1:60::/64 eq 5061 deny
udp any 2001:DB8:1:60::/64 eq 5060 deny udp any 2001:DB8:1:60::/64 eq 5061
deny tcp any 2001:DB8:1:60::/64 eq 5050 deny tcp any 2001:DB8:1:60::/64 eq
5620 ! !-- Permit other required traffic to the infrastructure address !--
range and allow IPv6 Neighbor Discovery packets, which !-- include Neighbor
Solicitation packets and Neighbor !-- Advertisement packets ! permit icmp any
any nd-ns permit icmp any any nd-na ! !-- Explicit deny for all other IP
traffic to the global !-- infrastructure address range ! deny ipv6 any
2001:DB8:1:60::/64 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic
!-- in accordance with existing security policies and configurations ! ! !--
Apply tACLs to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group 150 in ipv6 traffic-filter IPv6-
Infrastructure-ACL-Policy 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. Het genereren van deze berichten zou het ongewenste effect kunnen hebben van het verhogen van CPU-gebruik op het apparaat. 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 **zonder IP-onbereikbaar**. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met behulp van de **globale** configuratieopdracht **ip icmp-snelheidslimiet** *onbereikbaar interval-in-ms*.

Beperken: bescherming tegen spoofingUnicast doorsturen van omgekeerde paden De kwetsbaarheden die in dit document worden beschreven, kunnen worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast Reverse Path Forwarding (Unicast RPF) implementeren en configureren als een beschermingsmechanisme tegen spoofing.Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. Beheerders wordt aangeraden ervoor te zorgen dat de juiste Unicast RPF-modus (los of strikt) wordt geconfigureerd tijdens de implementatie van deze functie, omdat legitiem verkeer dat het netwerk oversteekt kan worden geminimaliseerd. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.Aanvullende informatie vindt u in de Unicast Reverse Path Forwarding Losse Mode functiehandleiding.Voor extra informatie over de configuratie en het gebruik van Unicast RPF, raadpleegt u het Witboek Understanding Unicast Reverse Path Forwarding Applied Intelligence.**IP-bronbeveiliging**IP Source Guard (IPSG) is een beveiligingsfunctie die IP-verkeer op niet-gerouteerde, Layer 2-interfaces beperkt door pakketten te filteren op basis van de bindende database met DHCP-snooping en handmatig ingestelde IP-bronbindingen. Beheerders kunnen IPSG gebruiken om aanvallen te voorkomen van een aanvaller die probeert pakketten te parasiteren door het IP-bronadres en/of het MAC-adres te vervalsen. Wanneer correct geïmplementeerd en geconfigureerd, biedt IPSG in combinatie met de strikte modus Unicast RPF de meest effectieve bescherming tegen spoofing voor de kwetsbaarheden die in dit document worden beschreven.Aanvullende informatie over de implementatie en configuratie van IPSG is te vinden in Configureren DHCP-functies en IP Source Guard.**Identificatie: Toegangscontrolelijsten voor douanevervoer**Nadat de beheerder de tACL op een interface heeft toegepast, zal de opdracht **IP-toegangslijsten** het aantal SIP- en SIP-TLS-pakketten op TCP- en UDP-poorten 5060 en 5061 identificeren die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te 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 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
```

```
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620
    70 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (5 matches)
    80 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (2 matches)
    90 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 (7 matches)
    100 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 (4 matches)
    110 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 (6 matches)
    120 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5620 (1 matches)
    130 permit icmp any any nd-ns
    140 permit icmp any any nd-ns
    150 deny ip any any
router#
```

In het voorafgaande voorbeeld, heeft toegangslijst 150 de volgende pakketten gelaten vallen die van een onbetrouwbare gastheer of een netwerk worden ontvangen:

- **5 SIP-**pakketten op **TCP-poort 5060** voor ACE-lijn 70
- **2 SIP-TLS-**pakketten op **TCP-poort 5061** voor ACE-lijn 80
- **7 SIP-**pakketten op **UDP-poort 5060** voor ACE-lijn 90
- **4 SIP-**pakketten op **UDP-poort 5061** voor ACE-lijn 100
- **6 SAF-**pakketten op **TCP-poort 5050** voor ACE-lijn 110
- **1 SAF-**pakket op **TCP-poort 5620** voor ACE-lijn 120

De bijbehorende output voor IPv6 tACL's lijkt erg op elkaar en wordt hier kort weggelaten. Voor extra informatie over het onderzoeken van incidenten met ACE-tellers en syslog-gebeurtenissen, raadpleegt u het white paper Identifying Incidents Use Firewall en IOS Router Syslog Events Applied Intelligence.Beheerders kunnen Embedded Event Manager gebruiken om instrumentatie te bieden wanneer aan specifieke voorwaarden is voldaan, zoals ACE-tellers. De Applied Intelligence white paper Embedded Event Manager in een security context biedt aanvullende informatie over hoe deze functie te gebruiken.**Identificatie: Vastlegging toegangslijst**De optie **log** en **log-input** toegangscontrolelijst (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 factoren die de CPU-impact van ACL-vastlegging bepalen, zijn loggeneratie, logtransmissie en processwitching naar voorwaartse pakketten die logbestanden met ACE's matchen.Voor Cisco IOS-software kan de opdracht **interval**-*in-ms* **vastlegging van IP-toegangslijst** 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.De CPU-impact van ACL-vastlegging kan worden aangepakt in hardware op de Cisco Catalyst 6500 Series-switches en Cisco 7600 Series-routers met Supervisor Engine 720 of Supervisor Engine 32 met behulp van geoptimaliseerde ACL-vastlegging.Voor extra informatie over de configuratie en het gebruik van ACL-vastlegging raadpleegt u het Witboek Inzicht in toegangscontrolelijst en toegepaste intelligentie.**Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding**Met Unicast RPF correct geïmplementeerd en geconfigureerd in de netwerkinfrastructuur, kunnen beheerders de *slot/poort* van het *type* show cef interface *gebruiken,* **ip interface tonen**, **cef drop tonen**, **ip cef switching statistieken tonen** en **ip traffic** opdrachten tonen om het aantal pakketten te identificeren dat Unicast RPF is gedaald. **Opmerking:** beginnend met Cisco IOS-softwareversie 12.4(20)T is de opdracht **tonen dat ip cef switching** is vervangen door **toon ip cef switching statistieken eigenschap**.**Opmerking: De show commando | begin** *regex* en **toon** *commando* **| omvat** *regex* commando modifiers worden gebruikt in de volgende voorbeelden om de hoeveelheid output te minimaliseren die beheerders moeten parseren om de gewenste informatie te bekijken. Er is aanvullende informatie over opdrachtbepalingen in de secties met de opdracht show van de opdrachtreferentie voor Cisco IOS Configuration Fundamentals.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop

  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

Opmerking: tonen cef interface *type sleuf / poort* **intern** is een verborgen opdracht die volledig moet worden ingevoerd op de opdrachtregel interface. Opdrachtvoltooiing is er niet voor beschikbaar.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
```

```
  IP verify source reachable-via RX, allow default, allow self-ping
  18 verification drops
  0 suppressed verification drops
router#


router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18           0           0
router#

router#show ip cef switching statistics feature
IPv4 CEF input features:
Path   Feature                Drop    Consume       Punt  Punt2Host Gave route
RP PAS uRPF                     18          0          0          0          0
Total                           18          0          0          0          0
    --      CLI Output Truncated       --
router#


router#show ip traffic | include RPF
         18 no route, 18 unicast RPF, 0 forced drop
router#
```

In de voorgaande **show cef drop**, **toon ip cef switching statistieken functie** en **toon ip traffic** voorbeelden, Unicast RPF heeft laten vallen **18 IP** pakketten die wereldwijd ontvangen zijn op alle interfaces met Unicast RPF geconfigureerd vanwege het onvermogen om het bronadres van de IP pakketten te verifiëren binnen de Forwarding Information Base van Cisco Express Forwarding.**Cisco IOS NetFlowIdentificatie: 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 mogelijk pogingen zijn om deze kwetsbaarheden te exploiteren. De beheerders worden geadviseerd om stromen te 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         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

In het vorige voorbeeld zijn er meerdere stromen voor SIP-, SAF- en SIP-TLS-pakketten op TCP-poorten 5060 (hex-waarde 13C4), 5061 (hex-waarde 13C5), 5050 (hex-waarde 13BA) en 5620 (hex-waarde 15F4) en UDP-poorten 5060 (hex-waarde 13C4) en **5061 (hex-waarde 1** .Dit verkeer wordt afkomstig van en verzonden naar adressen binnen het 192.168.60.0/24 adresblok, dat door getroffen apparaten wordt gebruikt. De pakketten in deze stromen kunnen worden gespoofd en kunnen wijzen op een poging om deze kwetsbaarheden te exploiteren. De beheerders worden geadviseerd om deze stromen bij basislijngebruik voor SIP en SIP-TLS verkeer te vergelijken dat op UDP-poorten 5060 en 5061 wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij afkomstig zijn van onbetrouwbare hosts of netwerken.Als u alleen de verkeersstromen voor SIP-, SAF- en SIP-TLS-pakketten op TCP-poorten 5060 (hex-waarde 13C4), 5061 (hex-waarde 13C5), 5050 (hex-waarde 13BA) en 5620 (hex-waarde 15F4) wilt weergeven, **toont** de opdracht **ip-cachestroom | neem SrcIf|_06_.*(13C4|13C5|13BA|15F4)_** zal de verwante UDP NetFlow-records weergeven zoals hier wordt getoond:**TCP-stromen**

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
router#
```

Als u alleen de verkeersstromen voor SIP- en SIP-TLS-pakketten op UDP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) wilt weergeven, **toont** de opdracht **de IP-cachestroom | neem SrcIf|_11_.*(13C4|13C5)_** zal de verwante verslagen van UDP NetFlow zoals hier getoond tonen:**UDP-stromen**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
router#
```

Identificatie: Traffic Flow Identification met IPv6 NetFlow-records Beheerders kunnen Cisco IOS IPv6 NetFlow op Cisco IOS-routers en -switches configureren als hulp bij de identificatie van verkeersstromen die kunnen worden geprobeerd te profiteren van de kwetsbaarheden die in dit document worden beschreven. De beheerders worden geadviseerd om stromen te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.Deze uitgang is afkomstig van een Cisco IOS-apparaat waarop Cisco IOS-software 12.4 hoofdlijn wordt uitgevoerd. De opdrachtsyntaxis varieert voor verschillende Cisco IOS-softwaretrainen.

```
router#show ipv6 flow cache
IP packet size distribution (50078919 total packets):
   1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
```

```
   .000 .990 .001 .008 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 475168 bytes
  8 active, 4088 inactive, 6160 added
  1092984 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  IP Sub Flow Cache, 33928 bytes
  16 active, 1008 inactive, 12320 added, 6160 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...6A:5BA6 Gi0/0    2001:DB...28::21 Gi0/1    0x3A 0x0000 0x8000 2191
2001:DB...6A:5BA6 Gi0/0    2001:DB...134::3 Gi0/1    0x3A 0x0000 0x8000 1909
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x3A 0x0000 0x8000 1192
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x3A 0x0000 0x8000 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...146::3 Gi0/1    0x3A 0x0000 0x8000 1392
2001:DB...6A:5BA6 Gi0/0    2001:DB...144::4 Gi0/1    0x3A 0x0000 0x8000 1493
```

Om weergave van het volledige 128-bits IPv6-adres toe te staan, gebruikt u de opdracht **eindbreedte 132** exec-modus.In het vorige voorbeeld zijn er meerdere stromen voor SIP-, SAF- en SIP-TLS-pakketten op TCP-poorten 5060 (hex-waarde 13C4), 5061 (hex-waarde 13C5), 5050 (hex-waarde 13BA) en 5620 (hex-waarde 15F4) en UDP-poorten 5060 (hex-waarde 13C4) en **5061 (hex-waarde 1** .Dit verkeer is afkomstig van en verzonden naar adressen binnen het adresblok 2001:DB8:1:60::/64, dat door getroffen apparaten wordt gebruikt. De pakketten in deze stromen kunnen worden gespoofd en kunnen wijzen op een poging om deze kwetsbaarheden te exploiteren. De beheerders worden geadviseerd om deze stromen bij basislijngebruik voor SIP en SIP-TLS verkeer te vergelijken dat op UDP-poorten 5060 en 5061 wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij afkomstig zijn van onbetrouwbare hosts of netwerken.Zoals in het volgende voorbeeld wordt getoond, om alleen de SIP-, SAF- en SIP-TLS-pakketten op TCP-poorten 5060 (hex-waarde 13C4), 5061 (hex-waarde 13C5), 5050 (hex-waarde 13BA) en 5620 (hex-waarde 15F4) te bekijken, gebruikt u de **show ipv6 flow cache | inclusief SrcAddress|_06_.*(13C4|13C5|13BA|15F4)_** opdracht om de gerelateerde NetFlow-records weer te geven:**TCP-stromen**

```
router#show ipv6 flow cache | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0 2001:DB...128::3 Gi0/1 0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
router#
```

Zoals in het volgende voorbeeld wordt getoond, kunt u alleen de verkeersstromen van SIP en SIP-TLS voor IPv6 UDP-poorten 5060 **(hex-waarde 0x13C4)** en 5061 **(hex-waarde 0x13C5)**gebruiken in het **cachegeheugen van** de **ipv6-stroom | inclusief SrcAddress|_11_.*(13C4|13C5)_** opdracht om de gerelateerde NetFlow-records weer te geven:**UDP-stromen**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
routter#
```

Cisco ASA- en FWSM-firewalls **Beperking: toegangscontrolelijsten voor douanevervoer**Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten die internetverbindingspunten, partner- en leverancierverbindingen of VPN-verbindingspunten kunnen omvatten, wordt beheerders aangeraden om tACL's te 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. Een tACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheden bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.Het tACL-beleid ontkent onbevoegde SIP-, SAF- en SIP-TLS-pakketten op TCP- en UDP-poorten 5060 en 5061 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 en 2001:DB8:1:60:/64 is de IPv4 en IPv6 adresruimte, respectievelijk, die wordt gebruikt door de getroffen apparaten, en de host op 192.168.100.1 (2001:DB8:1:100:1) wordt beschouwd als een vertrouwde bron die toegang tot de getroffen 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 tACL's staat in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable protocols and ports ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5620 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5620 ! !-- Permit or 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 tACL-Policy extended deny ip any any ! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable protocols and ports ! ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5050 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5620 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5050 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5620 ! !-- 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 ! ipv6 access-list IPv6-Transit-ACL-Policy deny ip any any ! !-- Apply tACLs to interfaces in the ingress direction ! access-group tACL-Policy in interface outside access-group IPv6-Transit-ACL-Policy in interface outside
```

Beperking: bescherming tegen spoofing met Unicast Reverse Path Forwarding De kwetsbaarheden die in dit document worden beschreven, kunnen worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast RPF implementeren en configureren als een beschermingsmechanisme tegen spoofing.Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast

RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en bij de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.Voor extra informatie over de configuratie en het gebruik van Unicast RPF, raadpleegt u de Cisco Security Appliance Command Reference voor IP-verificatie van het omgekeerde pad en het Understanding Unicast Reverse Path Forwarding Applied Intelligence-witboek.**Beperken: TCP-normalisatie**De TCP-normalisatiefunctie identificeert abnormale pakketten waarop het security apparaat kan reageren wanneer ze worden gedetecteerd; het security apparaat kan bijvoorbeeld de pakketten toestaan, laten vallen of wissen. De TCP-normalizer bevat niet-configureerbare acties en configureerbare acties. Meestal zijn niet-configureerbare acties die verbindingen laten vallen of verwijderen van toepassing op pakketten die als kwaadaardig worden beschouwd. TCP-normalisatie is beschikbaar vanaf softwarerelease 7.0(1) voor Cisco ASA 5500 Series adaptieve security applicatie en in softwarerelease 3.1(1) voor de Firewall Services module.TCP-normalisatie is standaard ingeschakeld en laat pakketten vallen die deze kwetsbaarheden kunnen uitbuiten. De bescherming tegen pakketten die deze kwetsbaarheid kunnen exploiteren is een niet configureerbare actie van de normalisatie van TCP geen configuratieveranderingen worden vereist om deze functionaliteit toe te laten.De normalisatiefunctie van TCP kan worden gebruikt om de gelijktijdige verbindingslimiet en de onbelaste time-out voor TCP-verbindingen met Cisco Unified Communications Manager te beperken en zo de DoS-voorwaarde te voorkomen. De beperkingen moeten worden geconfigureerd volgens het maximale normale aantal verbindingen dat naar de Cisco Unified Communications Manager is waargenomen. De lezer dient er rekening mee te houden dat het configureren van de TCP-normalisator om een abnormaal aantal verbindingen met de Cisco Unified Communications Manager te voorkomen, niet zal voorkomen dat een aanhoudende aanvaller het toegestane aantal verbindingen uitput, maar wel zal voorkomen dat de geheugen van Cisco Unified Communications Manager opraakt als gevolg van de vele inactieve verbindingen.**Opmerking:** de limieten die in elke omgeving zijn ingesteld, moeten voorzichtig zijn, omdat ze legitieme verbindingen kunnen ontkennen als ze niet zijn ingesteld om zich te houden aan de legitieme limieten voor de specifieke omgeving.In het volgende voorbeeld is 192.168.60.200/24 het IP-adres van het betreffende apparaat. De configuratie beperkt de gelijktijdige TCP-verbindingen tot het apparaat tot 1000 en stelt de verbinding met de inactiviteitstimer in op 30 minuten. Er moet voorzichtig worden omgegaan met de limieten die in elke omgeving worden gesteld, aangezien zij legitieme verbindingen kunnen ontkennen als zij niet zijn ingesteld om de normale limieten voor de specifieke omgeving te respecteren.

```
! !-- Match TCP traffic to the Cisco Unified Communications Manager ! access-list CVE-2011-2560-acl extended permit tcp any host 192.168.60.200 class-map CVE-2011-2560-cm match access-list CVE-2011-2560-acl ! !-- Configure the connection limits for TCP !-- traffic to the Cisco Unified Communications Manager ! policy-map global_policy class CVE-2011-2560-cm set connection conn-max 1000 set connection timeout idle 0:30:00 service-policy global_policy global
```

Aanvullende informatie over TCP-normalisatie vindt u in de sectie Configuration TCP Normalization van de Cisco ASA 5500 Series Configuration Guide in de CLI, 8.2.**Identificatie: Toegangscontrolelijsten voor douanevervoer**Nadat tACL is toegepast op een interface, kunnen beheerders de opdracht **show access-list** gebruiken om het aantal SIP- en SIP-TLS-pakketten op TCP- en UDP-poorten 5060 en 5061 te identificeren die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont toegang-lijst aan ACL-Beleid** volgt:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 9 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=34)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=24)
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=4)
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=44)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=61)
access-list tACL-Policy line 7 extended deny tcp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=5)
access-list tACL-Policy line 8 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
```

```
access-list tACL-Policy line 9 extended deny udp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=7)
access-list tACL-Policy line 10 extended deny udp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=4)
access-list tACL-Policy line 11 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5050 (hitcnt=6)
access-list tACL-Policy line 12 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5620 (hitcnt=1)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=8)
firewall#
```

In het voorafgaande voorbeeld, heeft de toegangslijst *tACL-Policy* de volgende pakketten die van een onbetrouwbare host of een onbetrouwbaar netwerk zijn ontvangen, verbroken:

- **5 SIP-**pakketten op **TCP-poort 5060** voor ACE-lijn 7
- **2 SIP-TLS-**pakketten op **TCP-poort 5061** voor ACE-lijn 8
- **7 SIP-**pakketten op **UDP-poort 5060** voor ACE-lijn 9
- **4 SIP-**pakketten op **UDP-poort 5061** voor ACE-lijn 10
- **6 SAF-**pakketten op **TCP-poort 5050** voor ACE-lijn 11
- **1 SAF-**pakketten op **TCP-poort 5620** voor ACE-lijn 12

De overeenkomstige output voor IPv6 tACLs is zeer gelijkaardig en zal hier voor beknoptheid worden weggelaten.**Identificatie: berichten in Firewall Access List System**Firewallsyslog-bericht *106023* wordt gegenereerd voor pakketten die worden geweigerd door een toegangscontrole-ingang (ACE) die niet het trefwoord voor het **logbestand** heeft. Aanvullende informatie over dit syslogbericht wordt weergegeven in Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106023.Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie is beschikbaar in Monitoring - Configuration Logging. De informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers is beschikbaar in Monitoring the Firewall Services Module.In het volgende voorbeeld, de **show vastlegging | grep** *regex* 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 te vinden in Create a Regular Expression.

```
firewall#show logging | grep 106023
  Aug 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2924
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.19/2934
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/3961
         dst inside:192.168.60.197/5050 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.201/2939
         dst inside:192.168.60.185/5620 by access-group "tACL-Policy"
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL *tACL-Policy zijn* geregistreerd mogelijk gespoofde **SIP- en SIP-TLS-**pakketten voor **TCP- en UDP-poorten 5060 en 5061** die naar het adresblok zijn verzonden dat aan de betreffende apparaten is toegewezen.Aanvullende informatie over syslogberichten voor ASA-beveiligingsapparaten is te vinden in Cisco ASA 5500 Series systeemlogberichten, 8.2. Aanvullende informatie over syslog-berichten voor de FWSM is te vinden in Catalyst 6500 Series Switch en Cisco 7600 Series router Firewall Services Module Logging System Berichten.Voor extra informatie over het onderzoeken van incidenten met behulp van syslog-gebeurtenissen, raadpleegt u het white paper Identifying Incidents Using Firewall en IOS Router Syslog Events Applied Intelligence.**Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding** Firewallsyslog-bericht *106021* wordt gegenereerd voor pakketten die worden geweigerd door Unicast PDF. Aanvullende informatie over dit syslogbericht wordt weergegeven in Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106021.Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie is beschikbaar in Monitoring - Configuration Logging. De informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600

Series routers is beschikbaar in Monitoring the Firewall Services Module.In het volgende voorbeeld, de **show vastlegging | grep** *regex* 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 te vinden in Create a Regular Expression.

```
firewall#show logging | grep 106021
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
```

De opdracht **Snel** starten tonen kan ook het aantal pakketten identificeren dat de Unicast RPF-functie is gevallen, zoals in het volgende voorbeeld:

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed                      11
firewall#
```

In het voorafgaande voorbeeld heeft Unicast RPF **11 IP-pakketten** laten vallen die zijn ontvangen op interfaces met Unicast RPF geconfigureerd. Het ontbreken van uitvoer geeft aan dat de Unicast RPF-functie op de firewall geen pakketten heeft laten vallen.Voor extra informatie over het debuggen van versnelde security pad gedropte pakketten of verbindingen, verwijzen we naar de Cisco Security Appliance Command Reference voor show asp drop.**Identificatie: TCP-normalisatie**Voor de Cisco ASA 5500 Series adaptieve security applicatie kan de opdracht **show service policy** het aantal pakketten identificeren dat de TCP-normalisatiefunctie is gedaald, zoals in het volgende voorbeeld:

```
firewall#  show service-policy set connection detail

Global policy:
  Service-policy: global_policy
    Class-map: CVE-2011-2560-cm
      Set connection policy: conn-max 1000
        current conns 15, drop 5
      Set connection timeout policy:
        idle 0:30:00
        DCD: disabled, retry-interval 0:00:15, max-retries 5
        DCD: client-probe 0, server-probe 0, conn-expiration 0            11
firewall#
```

In het vorige voorbeeld, heeft de normalisatie van TCP **5 nieuwe verbindingen** gedaald die de verbindingsgrens overschreden.

Cisco ACEBeperken: TCP-normalisatieTCP-normalisatie is een Layer 4-functie die bestaat uit een reeks controles die Cisco ACE uitvoert in verschillende fasen van een stroom, vanaf de eerste verbindingsinstelling tot en met het sluiten van een verbinding. Veel van de segmentcontroles kunnen worden gecontroleerd of gewijzigd door een of meer geavanceerde TCP-verbindingsinstellingen te configureren. ACE gebruikt deze TCP-verbindingsinstellingen om te beslissen welke controles moeten worden uitgevoerd en of een TCP-segment moet worden verworpen op basis van de resultaten van de controles. Het ACE verwerpt segmenten die abnormaal of misvormd lijken te zijn.TCP-normalisatie is standaard ingeschakeld en laat pakketten vallen die deze kwetsbaarheden kunnen uitbuiten. De bescherming tegen pakketten die deze kwetsbaarheid kunnen exploiteren is een niet configureerbare normalisatieactie van TCP; geen configuratieveranderingen worden vereist om deze functionaliteit toe te laten.De normalisatiefunctie van TCP kan worden gebruikt om de gelijktijdige verbindingslimiet, de verbindingssnelheid en de inactiviteitstimer voor TCP-verbindingen te beperken tot de Cisco Unified Communications Manager, en zo de DoS-voorwaarde te voorkomen. De beperkingen moeten worden geconfigureerd volgens het maximale normale aantal en tarief van verbindingen dat naar Cisco Unified Communications Manager is waargenomen. De lezer dient er rekening mee te houden dat het configureren van de TCP-normalisator om een abnormaal aantal verbindingen met de Cisco Unified Communications Manager te voorkomen, niet zal voorkomen dat een aanhoudende aanvaller het toegestane aantal verbindingen uitput, maar wel zal voorkomen dat de geheugen van Cisco Unified Communications Manager opraakt als gevolg van de vele inactieve verbindingen.**Opmerking:** de limieten die in elke omgeving zijn ingesteld, moeten voorzichtig zijn, omdat ze legitieme verbindingen kunnen ontkennen als ze niet zijn ingesteld om zich te houden aan de legitieme limieten voor de specifieke omgeving.In het volgende voorbeeld is 192.168.60.200/24 het IP-adres van het betreffende apparaat. De configuratie beperkt de gelijktijdige TCP-verbindingen tot het apparaat tot 1000 en de verbindingssnelheid tot 100000 verbindingen per seconde. De time-out voor de verbinding wordt ingesteld op 30 minuten.

```
! !-- Create a connection parameter map to group together TCP/IP !--
normalization and termination parameters ! parameter-map type connection CVE-
2011-2560-parameter-map limit-resource conc-connections 1000 set timeout
inactivity 1800 rate-limit connection 100000 ! !-- Match TCP traffic to the
Cisco Unified Communications Manager ! class-map match-any CVE-2011-2560-cm
match destination-address 192.168.60.200 ! !-- Configure the connection
limits for TCP !-- traffic to the Cisco Unified Communications Manager !
policy-map multi-match CVE-2011-2560_policy class CVE-2011-2560-cm connection
advanced-options CVE-2011-2560-parameter-map ! !-- Apply the policy to the
interface ! interface vlan 50 service-policy input CVE-2011-2560_policy
```

Aanvullende informatie over TCP-normalisatie vindt u in het gedeelte TCP/IP-normalisatie en IP-herassemblageparameters configureren van de configuratiehandleiding voor applicatie van Cisco ACE 4700 Series.**Identificatie: TCP-normalisatie**De Cisco ACE-applicatie en module voor Application Control Engine bieden geen uitvoer van tonen voor pakketten die zijn gedropt terwijl ze deze kwetsbaarheden proberen te exploiteren.**Cisco-inbraakpreventiesysteem****Beperken: acties voor Cisco IPS-handtekeningen**Beheerders kunnen Cisco Inbraakpreventiesysteem (IPS) gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om een van de kwetsbaarheden te exploiteren die in dit document worden beschreven. Beginnend met handtekeningsupdate S590 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kan de kwetsbaarheid worden gedetecteerd door handtekening 38386/0(Handtekeningnaam: Cisco Intercompany Media Engine Denial of Service). Signature 38386/0 is standaard ingeschakeld, activeert een *Medium* Severity event, heeft een Signature Fidelity Rating (SFR) van 15 en is geconfigureerd met een default event action **van Produce Alert**.De branden van de handtekening 38386/0 wanneer specifieke kwaadwillige pakketten die met TCP-poort 5620 worden verzonden worden ontdekt. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.Beheerders kunnen Cisco IPS-sensoren configureren om een gebeurtenisactie uit te voeren wanneer een aanval wordt gedetecteerd. De geconfigureerde gebeurtenisactie voert preventieve of afschrikkende controles uit om te helpen beschermen tegen een aanval die probeert de kwetsbaarheden te exploiteren die in dit document worden beschreven.Explosies die gespoofde IP-adressen gebruiken kunnen ervoor zorgen dat een geconfigureerde gebeurtenisactie per ongeluk verkeer van vertrouwde bronnen ontkent.Cisco IPS-sensoren zijn het meest effectief wanneer ze worden ingezet in inline beschermingsmodus in combinatie met het gebruik van een gebeurtenisactie. Automatische bedreigingspreventie voor Cisco IPS 6.x en grotere sensoren die in de modus voor inline bescherming worden geïmplementeerd, biedt bedreigingspreventie tegen een aanval die probeert de kwetsbaarheden te exploiteren die in dit document worden beschreven. De preventie van de bedreiging wordt bereikt door een standaardopheffing die een gebeurtenisactie voor teweeggebrachte handtekeningen met een *riskRatingValue* groter dan 90 uitvoert.Voor aanvullende informatie over de risicorating en de berekening van de dreigingswaardering, de referentie Risicorating en de dreigingswaardering: Vereenvoudig IPS-beleidsbeheer.**Cisco-systeem voor beveiligingsbewaking, analyse en respons****Identificatie: incidenten van Cisco-systeem voor beveiligingsbewaking, analyse en respons**Het apparaat Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan incidenten veroorzaken met betrekking tot gebeurtenissen die zijn gerelateerd aan de kwetsbaarheden die in dit document worden beschreven met behulp van IPS-handtekeningen 38386/0 (Handtekeningnaam: Cisco Intercompany Media Engine Denial of Service). Nadat de S590 dynamische handtekeningupdate is gedownload, met behulp van sleutelwoord **NR-38386/0** voor IPS-handtekening 38386/0 en een vraagtype van **< Alle overeenkomende gebeurtenissen | Alle Raw-berichten voor** overeenkomende gebeurtenissen**>** op het Cisco Security MARS-apparaat bevatten een rapport met de incidenten die met de IPS-handtekening zijn gemaakt.Beginnend met de versies 4.3.1 en 5.3.1 van Cisco Security MARS-apparaten, is de ondersteuning voor de functie van Cisco IPS dynamische handtekeningen toegevoegd. Deze functie downloadt nieuwe handtekeningen van Cisco.com of van een lokale webserver, verwerkt en categoriseert correct ontvangen gebeurtenissen die overeenkomen met die handtekeningen, en omvat ze in inspectieregels en rapporten. Deze updates bieden normalisatie van gebeurtenissen en gebeurtenisgroepstoewijzing, en ze stellen ook het MARS-apparaat in staat om nieuwe handtekeningen van de IPS-apparaten te parseren.**Waarschuwing:** als dynamische handtekeningupdates niet zijn geconfigureerd, worden gebeurtenissen die deze nieuwe handtekeningen weergeven als *onbekend gebeurtenistype* in vragen en rapporten. Omdat MARS deze gebeurtenissen niet opneemt in de inspectieregels, kunnen incidenten niet worden gecreëerd voor potentiële bedreigingen of aanvallen die binnen het netwerk plaatsvinden.Deze optie is standaard ingeschakeld, maar moet geconfigureerd worden. Als deze niet is geconfigureerd, wordt de volgende Cisco Security MARS-regel geactiveerd:

```
System Rule: CS-MARS IPS Signature Update Failure
```

Wanneer deze functie is ingeschakeld en geconfigureerd, kunnen beheerders de huidige handtekeningsversie bepalen die door MARS is gedownload door **Help >** About te selecteren en de waarde voor *IPS Signature Version* te bekijken.Er is aanvullende informatie over updates van dynamische handtekeningen en instructies voor het configureren van dynamische handtekeningupdates beschikbaar voor de releases van Cisco Security MARS 4.3.1 en 5.3.1.

Aanvullende informatie

DIT DOCUMENT WORDT AANGEBODEN OP EEN ‘AS IS’-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIP VAN GARANTIES VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. UW GEBRUIK VAN DE INFORMATIE IN HET DOCUMENT OF DE MATERIALEN GEKOPPELD AAN HET DOCUMENT IS GEHEEL OP EIGEN RISICO. CISCO BEHOUDT ZICH HET RECHT VOOR OM DIT DOCUMENT TE ALLEN TIJDE TE WIJZIGEN OF TE ANNULEREN.

Revisiegeschiedenis

Revisie 1.1	2011-12 november-2	Correcte document-URL
Revisie 1.0	2011-augustus-24	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
- Cisco-beveiliging
- Cisco Security IntelliShield Alert Manager-service
- Cisco-handleiding over het versterken van Cisco IOS-apparaten
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- NetFlow-prestatieanalyse
- Witboeken voor Cisco Network Foundation-bescherming
- Cisco Firewallproducten - startpagina op Cisco.com
- Cisco ACE-documentatie voor Application Control Engine
- Verbeteringen in Unicast Reverse Path Forwarding voor de Internet Service Provider
- Cisco-inbraakpreventiesysteem
- Cisco-downloads voor IPS-handtekeningen
- Cisco-zoekpagina voor IPS-handtekeningen
- Cisco-systeem voor beveiligingsbewaking, analyse en respons
- Gemeenschappelijke kwetsbaarheden en blootstellingen (CVE)

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.