Identificatie en beperking van exploitatie van meerdere VoS-kwetsbaarheden in Cisco Unified Communications-producten

Identificatie en beperking van exploitatie van meerdere VoS-kwetsbaarheden in Cisco Unified Communications-producten

Advies-ID: cisco-amb-20100825-cucm-cup

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100825-cucm-cup

Revisie 1.0

2010 augustus 25 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit bulletin voor toegepaste beperking is een begeleidend document voor de PSIRT Security Advisories Cisco Unified Communications Manager Denial of Service Vulnerabilities en Cisco Unified Presence Denial of Service Vulnerabilities en biedt identificatie- en onderdrukkingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in het SIP-proces van de Cisco Unified Communications Manager en Cisco Unified Presence-producten. De volgende subsecties vatten deze kwetsbaarheden samen:

Kwetsbaarheden Cisco Unified Communications Manager Denial of Service (Dos): deze kwetsbaarheden kunnen op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheden kan resulteren in een denial of

service (DoS)-conditie. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheden kunnen resulteren in een aanhoudende DoS-conditie.

De aanvalsvectoren voor exploitatie worden via SIP-pakketten met behulp van de volgende protocollen en poorten:

- SIP met TCP-poort 5060
- SIP met TCP-poort 5061
- SIP met UDP-poort 5060
- SIP met UDP-poort 5061

Een aanvaller kon deze kwetsbaarheden exploiteren met gespoofde pakketten.

Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2010-2837 en CVE-2010-2838.

Kwetsbaarheid door Cisco Unified Presence Denial of Service (DoS): deze kwetsbaarheden kunnen op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheden kan resulteren in een denial of service (DoS)-conditie. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheden kunnen resulteren in een aanhoudende DoS-conditie.

De aanvalsvectoren voor exploitatie worden via SIP-pakketten met behulp van de volgende protocollen en poorten:

- SIP met TCP-poort 5060
- SIP met TCP-poort 5061
- SIP met UDP-poort 5060
- SIP met UDP-poort 5061

Een aanvaller kon deze kwetsbaarheden exploiteren met gespoofde pakketten.

Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2010-2839 en CVE-2010-2840.

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-20100825-cucm en https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100825-cup.

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.

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.

- TACL's
- Unicast RPF

Deze beschermingsmechanismen filteren en vallen, evenals verifiëren het bron IP adres van, pakketten die proberen om 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 en FWSM firewalls kunnen zichtbaarheid bieden door syslog-berichten 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 hun standaard risicobeoordelings- en risicobeperkingsprocessen te volgen om de potentiële impact 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 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-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-pakketten op TCP-poorten 5060 en 5061 en UDP-poorten 5060 en 5061 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP 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 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 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 ! !-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks ! access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
5061 access-list 150 deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny
udp any 192.168.60.0 0.0.0.255 eq 5061 ! !-- 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 ! !--
Apply tACL to interfaces 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. 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 **algemene** opdracht voor configuratie **ip icmp-snelheidslimiet voor onbereikbare** *interval-in-ms*.

Beperken: bescherming tegen spoofing

Unicast 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-pakketten op TCP-poorten 5060 en 5061 en UDP-poorten 5060 en 5061 die zijn gefilterd, identificeren. 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 (1 match)
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (31 matches)
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 (15 matches)
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (5 matches)
    50 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (227 matches)
    60 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (257 matches)
```

```
70 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (130 matches)
80 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (175 matches)
90 deny ip any any (5219 matches)
```

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

- **227 SIP**-pakketten op **TCP-poort 5060** voor ACE-lijn 50
- **257 SIP**-pakketten op **TCP-poort 5061** voor ACE-lijn 60
- **130 SIP**-pakketten op **UDP-poort 5060** voor ACE-lijn 70
- **175 SIP**-pakketten op **UDP-poort 5061** voor ACE-lijn 80

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: het vastleggen van toegangscontrolelijsten 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 *sleuf/poort* van het *type* show cef-interface *intern* 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 *opdracht* **show** | **begin met** *regex* en **toon** *opdracht* | **omvat** *regex* commando modifiers worden gebruikt in de volgende voorbeelden om de hoeveelheid output te minimaliseren die beheerders zullen 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 globaal ontvangen 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 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 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 (54955 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .082 .531 .375 .000 .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 .009 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  167 active, 3929 inactive, 32741 added
  607632 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 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-WWW            109      0.0         3    40      0.0       0.0      15.4
TCP-BGP          28425      0.0         1    68      0.0       2.9      15.4
TCP-other         1111      0.0         6    40      0.0       0.0      15.4
UDP-NTP           2221      0.0         1    76      0.0       0.0      15.6
UDP-TFTP            95      0.0         4    28      0.0       0.0      15.6
UDP-other          589      0.0         6    28      0.0       0.0      15.4
ICMP                24      0.0        31  1009      0.0      19.9      15.4
Total:           32574      0.0         1    75      0.0       2.5      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.68.44   Et0/1         192.168.60.212  06 F208 098B     4
Et0/0         192.168.38.121  Et0/1         192.168.60.6    06 A826 01BB     3
Et0/0         192.168.224.241 Et0/1         192.168.60.182  06 7536 13C5     5
Et0/0         192.168.212.211 Et0/1         192.168.60.114  06 AB5E 01BB     2
Et0/0         192.168.205.69  Et0/1         192.168.60.110  06 98A5 0ABC    10
Et0/0         192.168.40.45   Et0/1         192.168.60.42   06 5FA7 01BB     2
Et0/0         192.168.4.192   Et0/1         192.168.93.248  11 FFFE 8002    15
Et0/0         192.168.44.66   Et0/1         192.168.178.29  06 A30D 0F4A     3
Et0/0         192.168.36.239  Et0/1         192.168.60.214  11 BCA3 0045     3
Et0/0         192.168.60.164  Et0/1         192.168.60.26   11 1EFB 13C4     2
Et0/0         192.168.234.206 Et0/1         192.168.147.20  11 C959 9972    17
Et0/0         192.168.148.143 Et0/1         192.168.60.25   11 CD48 0045     2
Et0/0         192.168.250.187 Et0/1         192.168.60.41   06 C5B3 098B     3
Et0/0         192.168.227.167 Et0/1         192.168.125.75  06 1048 23FC     3
Et0/0         192.168.107.126 Et0/1         192.168.194.53  06 3767 139B    13
Et0/0         192.168.1.194   Et0/0         192.168.60.155  06 CE95 098B   192
Et0/0         192.168.118.14  Et0/1         192.168.226.46  11 3966 FF31     8
Et0/0         192.168.35.154  Et0/1         192.168.60.77   06 3C5C 0ABC     1
Et0/0         192.168.145.167 Et0/1         192.168.60.74   11 B06D 0045     7
Et0/0         192.168.56.109  Et0/1         192.168.247.33  11 3F4C 9E2C     6
Et0/0         192.168.28.223  Et0/1         192.168.60.154  06 B35D 13C4     1
Et0/0         192.168.139.201 Et0/1         192.168.60.229  06 8E56 07D0     2
Et0/0         192.168.60.199  Et0/1         192.168.60.242  11 37AF 13C4     5
Et0/0         192.168.212.244 Et0/1         192.168.59.244  06 9CB9 95F7    12
Et0/0         192.168.133.250 Et0/1         192.168.60.49   06 41A2 098B     4
Et0/0         192.168.92.118  Et0/1         192.168.13.136  11 82E2 95B8     2
Et0/0         192.168.206.122 Et0/1         192.168.54.12   06 A09B 7514    11
Et0/0         192.168.164.86  Et0/1         192.168.60.44   11 4ED8 0045     7
Et0/0         192.168.144.222 Et0/1         192.168.60.188  06 770C 13C4     1
Et0/0         192.168.138.85  Et0/1         192.168.60.38   11 9B7D 13C4    11
Et0/0         192.168.185.139 Et0/1         192.168.97.208  11 A25E FE8C     8
```

```
Et0/0         192.168.78.45   Et0/1          192.168.92.184  11 08B5 BD08    13
Et0/0         192.168.2.81    Et0/1          192.168.60.138  11 3258 13C5     2
Et0/0         192.168.144.96  Et0/1          192.168.99.50   06 9D6D 4E7E    15
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor SIP op TCP (Protocol hex waarde 06) poorten 5060 (hex waarde 13C4) en 5061 (hex waarde 13C5) en UDP (Protocol hex waarde 11) poorten **5060 (hex waarde 13C4)** en **5061 (hex waarde 13C5)**.

Een deel van dit verkeer is 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 verkeer te vergelijken dat op TCP-poorten 5060 en 5061 en UDP-poorten 5060 en 5061 wordt verzonden, en ook de stromen te onderzoeken om te bepalen of zij afkomstig zijn van niet-vertrouwde hosts of netwerken.

Als u alleen de verkeersstromen voor SIP-pakketten wilt weergeven op TCP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) en UDP-poorten (Protocol hex-waarde 11) 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5), **tonen** de opdrachten **ip-cachestroomstroom | inclusief SrcIf**|*_06_.*(13C4|13C5)* en **toon ip cache flow | inclusief SrcIf**|*_11_.*(13C4|13C5)* zal de gerelateerde TCP- en UDP NetFlow-records weergeven zoals hier wordt getoond:

TCP-stromen

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.114.191 Et0/1          192.168.60.53   06 1713 13C4     4
Et0/0         192.168.40.246  Et0/1          192.168.60.145  06 CC2D 13C5     9
Et0/0         192.168.147.251 Et0/1          192.168.60.183  06 E2E1 13C4     1
Et0/0         192.168.88.150  Et0/1          192.168.60.197  06 6E1D 13C5    10
Et0/0         192.168.16.232  Et0/1          192.168.60.235  06 BD24 13C4     4
Et0/0         192.168.30.204  Et0/1          192.168.60.16   06 1A93 13C4     3
Et0/0         192.168.65.79   Et0/1          192.168.60.223  06 3FD5 13C5     2
Et0/0         192.168.82.123  Et0/1          192.168.60.100  06 ACA7 13C4     2
Et0/0         192.168.224.47  Et0/1          192.168.60.178  06 5BD7 13C4     3
Et0/0         192.168.87.54   Et0/1          192.168.60.49   06 D55B 13C5     2
router#
```

UDP-stromen

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.151.1   Et0/1          192.168.60.96   11 2C2D 13C5     3
Et0/0         192.168.237.123 Et0/1          192.168.60.131  11 5712 13C5     4
Et0/0         192.168.246.100 Et0/1          192.168.60.37   11 FCBC 13C5     4
Et0/0         192.168.126.21  Et0/1          192.168.60.103  11 9716 13C4     1
Et0/0         192.168.60.28   Et0/1          192.168.60.244  11 E40B 13C4   192
Et0/0         192.168.56.139  Et0/1          192.168.60.218  11 4EE8 13C4    10
Et0/0         192.168.51.212  Et0/1          192.168.60.209  11 835D 13C4     3
Et0/0         192.168.252.73  Et0/1          192.168.60.115  11 521E 13C4     3
router#
```

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-pakketten op TCP-poorten 5060 en 5061 en UDP-poorten 5060 en 5061 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP 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 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 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 ! !-- 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 ! !-- 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 ! !-- Apply tACL to interface(s) in the ingress
direction ! access-group tACL-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.

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders de **show access-list** opdracht gebruiken om het aantal SIP-pakketten op TCP-poorten 5060 en 5061 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=224)
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=28)
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=36)
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=41)
access-list tACL-Policy line 5 extended deny tcp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=78)
access-list tACL-Policy line 6 extended deny tcp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=39)
access-list tACL-Policy line 7 extended deny udp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=437)
access-list tACL-Policy line 8 extended deny udp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=478)
access-list tACL-Policy line 9 extended deny ip any any (hitcnt=563)
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:

- **78 SIP-**pakketten op **TCP-poort 5060 (SIP)** voor ACE-lijn 5
- **39 SIP-**pakketten op **TCP-poort 5061** voor ACE-lijn 6
- **437 SIP-**pakketten op **UDP-poort 5060 (SIP)** voor ACE-lijn 7
- **478 SIP-**pakketten op **UDP-poort 5061** voor ACE-lijn 8

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 04 2010 08:45:44: %ASA-4-106023: Deny tcp src outside:192.168.60.5/22724
            dst inside:192.168.60.21/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:44: %ASA-4-106023: Deny tcp src outside:192.168.0.4/40011
            dst inside:192.168.60.15/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:44: %ASA-4-106023: Deny tcp src
outside:192.168.208.144/61650
            dst inside:192.168.60.11/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src outside:192.168.0.2/59865
            dst inside:192.168.60.31/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src outside:192.168.48.42/12345

            dst inside:192.168.60.3/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src
outside:192.168.126.168/5053
            dst inside:192.168.60.9/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src
outside:192.168.60.134/22670
            dst inside:192.168.60.11/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src outside:192.168.44.68/18777

            dst inside:192.168.60.13/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src
outside:192.68.214.152/13391
            dst inside:192.168.60.41/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src outside:192.168.23.3/21826
            dst inside:192.168.60.10/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src
outside:192.168.34.173/29006
            dst inside:192.168.60.8/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src
outside:192.168.28.109/16289
            dst inside:192.168.60.99/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src outside:192.168.81.251/9919

            dst inside:192.168.60.1/5060 by access-group "tACL-Policy"
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL *tACL-Policy zijn* geregistreerd mogelijk gespoofde **SIP-**pakketten voor **TCP-poorten 5060 en 5061** 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 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.202 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.126 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.22 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.75 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.248 to 192.168.60.1 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 (rpf-violated)                    10
```

In het voorafgaande voorbeeld heeft Unicast RPF **10 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.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

Beheerders kunnen Cisco Inbraakpreventiesysteem (IPS) gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om de kwetsbaarheden te exploiteren die in dit document worden beschreven. Deze kwetsbaarheden kunnen worden gedetecteerd door de volgende handtekeningen:

- 29219-0 CUCM misvormd REGISTER Bericht DoS
- 29239-0 Cisco CUP-geheugen voor corruptiekwetsbaarheid

29219-0 CUCM misvormd REGISTER Bericht DoS

Beginnend met handtekeningsupdate S510 voor sensoren met Cisco IPS versie 6.x en hoger, kan deze kwetsbaarheid worden gedetecteerd door handtekening 29219/0 (Handtekeningnaam: CUCM Malform REGISTER Message DoS). Signature 29219/0 is standaard ingeschakeld, activeert een *Medium* Severity event, heeft een Signature Fidelity Rating (SFR) van 90 en is geconfigureerd met een default event action of **production-alert**.

Deze handtekening brandt op het detecteren van een misvormd SIP REGISTER-bericht dat een Denial of Service kan veroorzaken in Cisco Unified Communications Manager. De kwetsbaarheid is gedocumenteerd in Cisco bug-id CSCtf66305 en is toegewezen aan de CVE-identificatie CVE-2010-2838. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheid.

29239-0 Cisco CUP-geheugen voor corruptiekwetsbaarheid

Beginnend met handtekeningsupdate S510 voor sensoren met Cisco IPS versie 6.x en hoger, kan deze kwetsbaarheid worden gedetecteerd door handtekening 29239/0 (Handtekeningnaam: Cisco CUP Memory Corruption Vulnerability). Handtekening 29239/0 is standaard ingeschakeld, activeert een gebeurtenis met *hoge* ernst, heeft een SFR (Signature Fidelity Rating) van 90 en is geconfigureerd met een **waarschuwing voor** standaardgebeurtenissen.

Deze handtekening vuurt op pogingen om een geheugen corruptie bug aanwezig in Cisco CUP te exploiteren met behulp van TCP poort 5070. De kwetsbaarheid is gedocumenteerd in Cisco bug-id CSCtd39629 en is toegewezen aan de CVE-identificatie CVE-2010-2840. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheid.

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.

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 29219-0 (Signature Name: CUCM Malform REGISTER Message DoS) en 29239-0 (Signature Name: Cisco CUP Memory Corruption Vulnerability). Nadat de dynamische handtekeningupdate

S510 is gedownload, zal het gebruik van trefwoorden **NR-29219/0** voor IPS-handtekening 29219/0 en **NR-29239/0** voor IPS-handtekening 29239/0 en een vraagtype van **Alle overeenkomende onbewerkte berichten van de Gebeurtenis** op Cisco Security MARS applicatie een rapport verstrekken dat een lijst maakt van de incidenten die door 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 versie van handtekeningen die door MARS is gedownload, bepalen door **Help > Info** 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 1.0	2010-25 augustus	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
- De betekenis van cross-site scripting (XSS) bedreigingsvectoren
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- NetFlow-prestatieanalyse
- Witboeken voor Cisco Network Foundation-bescherming
- Presentaties voor Cisco Network Foundation-bescherming
- Identificatie en beperking van TTL-aanval bij verlopen
- Een security georiënteerde benadering van IP-adressering
- Tegenmaatregelen voor kwaadwillig gebruik van IPv6 Type 0-routingkoppen
- Cisco Firewallproducten - startpagina op Cisco.com
- 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.