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

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

Advies-ID: cisco-amb-20110427-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110427-cucm

Revisie 1.1

Openbare publicatie 2011 April 27 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document bij de PSIRT Security Advisory *Multiple Vulnerabilities in Cisco Unified Communications Manager* en biedt identificatie- en onderdrukkingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in Cisco Unified Communications Manager. De volgende subsecties vatten deze kwetsbaarheden samen:

Session Initiation Protocol (SIP) — Vulnerabilities voor serviceweigering**:** deze kwetsbaarheden kunnen op afstand worden geëxploiteerd zonder verificatie en zonder interactie van de eindgebruiker. Succesvolle benutting van deze kwetsbaarheden kan resulteren in een denial of service (DoS)-conditie.

De aanvalsvectoren voor exploitatie worden door pakketten gebruikt die de volgende protocollen en poorten gebruiken:

- 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-2011-1604, CVE-2011-1605 en CVE-2011-1606.

Cisco Unified Reporting Onbevoegde kwetsbaarheid voor uploaden van bestanden: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan een externe aanvaller toestaan om een kwaadaardig bestand te uploaden. De aanvalsvector voor exploitatie is via HTTPS-pakketten via TCP-poort 8443.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-1607.

Meervoudige SQL Injection Vulnerabilities: Deze kwetsbaarheden kunnen op afstand worden geëxploiteerd, met en zonder authenticatie, en zonder interactie van de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheden kan informatieonthulling toestaan, die een aanvaller in staat stelt om informatie over het getroffen apparaat te leren.

De aanvalsvectoren voor exploitatie worden door pakketten gebruikt die de volgende protocollen en poorten gebruiken:

- HTTP met TCP-poort 80
- HTTPS met TCP-poort 443
- HTTP met TCP-poort 8080
- HTTPS met TCP-poort 8443

Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2011-1609 en CVE-2011-1610.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory, die beschikbaar is via de volgende link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110427-cucm.

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- en UDP-poorten 5060 en 5061, HTTP-pakketten op TCP-poorten 80 en 8080 en HTTPS-pakketten op TCP-poorten 443 en 8443 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 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 80 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 443 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 ! !--
The following vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list 150 deny tcp any 192.168.60.0 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 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80 access-
list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 8080 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
8443 ! !-- 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 tonen** het aantal SIP-pakketten op TCP- en UDP-poorten 5060 en 5061, HTTP-pakketten op TCP-poorten 80 en 8080 en HTTPS-pakketten op TCP-poorten 443 en 8443 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
    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 80
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
    90 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (17 matches)
    100 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (19 matches)
    110 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (3 matches)
    120 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (49 matches)
    130 deny tcp any 192.168.60.0 0.0.0.255 eq 80 (32 matches)
    140 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (20 matches)
    150 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (35 matches)
    160 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (10 matches)
    170 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:

- **17 SIP-**pakketten op **TCP-poort 5060** voor ACE-lijn 90
- **19 SIP-**pakketten op **TCP-poort 5061** voor ACE-lijn 100
- **3 SIP-**pakketten op **UDP-poort 5060** voor ACE-lijn 110
- **49 SIP-**pakketten op **UDP-poort 5061** voor ACE-lijn 120
- **32 HTTP**-pakketten op **TCP-poort 80** voor ACE-lijn 130
- **20 HTTPS-**pakketten op **TCP-poort 443** voor ACE-lijn 140
- **35 HTTP**-pakketten op **TCP-poort 8080** voor ACE-lijn 150
- **10 HTTPS-**pakketten op **TCP-poort 8443** voor ACE-lijn 160

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 *sleuf/poort* van het *type* show cef *interfacetype 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* **|** *regex*-opdrachtwijzigingen **omvatten** die in de volgende voorbeelden worden gebruikt 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 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 (31715553 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .005 .175 .632 .032 .095 .003 .003 .003 .002 .000 .005 .002 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .020 .007 .008 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  24 active, 65512 inactive, 5451612 added
  557541771 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 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         811      0.0       137    41      0.0      32.3      16.4
TCP-FTP           2108      0.0         6    44      0.0       0.5      22.1
TCP-FTPD             5      0.0        13    52      0.0       0.7       1.5
TCP-WWW         133468      0.0         4   223      0.1       5.5      50.9
TCP-SMTP         32583      0.0         5    60      0.0      28.3      60.0
TCP-other       627608      0.1        12   175      1.8      57.8      24.1
UDP-DNS         284078      0.0         3    63      0.2      15.1      53.5
UDP-NTP          94456      0.0         1    76      0.0       0.3      60.5
UDP-Frag             1      0.0         9  1260      0.0       0.4      60.2
UDP-other      1102669      0.2         8   102      2.1      34.3      47.5
ICMP           1980458      0.4         2    89      1.1      14.3      58.5
IGMP            469264      0.1         2    37      0.2      58.2      41.0
IPINIP               2      0.0         1    76      0.0       0.0      60.4
IPv6INIP             3      0.0         1   863      0.0       0.0      60.4
GRE                  2      0.0         1   697      0.0       0.0      60.4
```

```
IP-other        724037      0.1         9    89      1.5      95.0      15.6
Total:         5451553      1.2         5   113      7.3      37.5      44.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  11 0984 00A1     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  11 0911 13C5     3
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   11 0B3E 13C4     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 13C4     1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
Gi0/0         192.168.120.20  Gi0/1         192.168.60.102  06 0984 1F90     1
Gi0/0         192.168.12.45   Gi0/1         192.168.60.138  06 0911 13C5     3
Gi0/1         192.168.150.41  Gi0/0         192.168.60.24   06 0016 12CA     1
Gi0/0         192.168.12.87   Gi0/1         192.168.60.28   06 0B3E 0050     5
Gi0/0         192.168.10.12   Gi0/1         192.168.60.97   06 0B89 01BB     1
Gi0/0         10.88.226.8     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.15   Gi0/1         192.168.60.209  06 0BD7 20FB     1
Gi0/0         10.89.16.216    Gi0/1         192.168.150.8   06 12CA 0016     1
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor SIP op TCP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) en UDP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) en HTTP op TCP-poorten 80 (hex-waarde 0050) en 8080 (hex-waarde 1F90) TCP-poorten 443 (hex-waarde 10B) en 8443 (hex-waarde 20FB).

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 verkeer te vergelijken dat op UDP-poort 5060 en poort 5061 wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij afkomstig zijn van onbetrouwbare hosts of netwerken.

Om alleen de verkeersstromen voor SIP-pakketten op UDP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) te bekijken, **toont** de opdracht **ip-cachestroom | inclusief SrcIf|** _11_.*(13C4|13C5) zal de gerelateerde UDP NetFlow-records weergeven zoals hier wordt getoond:

UDP-stromen

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.12.110   Gi0/1         192.168.60.163  11 092A 13C4     6
Gi0/0         192.168.11.230   Gi0/1         192.168.60.20   11 0C09 13C4     1
Gi0/0         192.168.11.131   Gi0/1         192.168.60.245  11 0B66 13C5    18
Gi0/0         192.168.13.7     Gi0/1         192.168.60.162  11 0914 13C4     1
router#
```

Als u alleen de verkeersstromen voor SIP-pakketten op TCP-poorten 5060 (hex-waarde 13C4) en 5061 (hex-waarde 13C5) en HTTP-pakketten op TCP-poorten 80 (hex-waarde 0050) en 8080 (hex-waarde 1F90) en HTTPS-pakketten op TCP-poorten 443 (hex-waarde 01BB) en 8443 (hex-waarde 20FB) wilt weergeven, **toont** de opdracht ip-cached-cachederstroom **| inclusief SrcIf|** _06_.*(13C4|13C5|0050|01B|1F90|20FB) geeft de gerelateerde TCP NetFlow-records weer zoals hier wordt getoond:

TCP-stromen

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB)
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.12.110   Gi0/1         192.168.60.163  06 092A 13C5     6
Gi0/0         192.168.11.230   Gi0/1         192.168.60.20   06 0C09 0050     1
Gi0/0         192.168.11.131   Gi0/1         192.168.60.245  06 0B66 01BB    18
Gi0/0         192.168.13.7     Gi0/1         192.168.60.162  06 0914 0050     7
Gi0/0         192.168.241.106  Gi0/1         192.168.60.27   06 0B7B 13C4    12
Gi0/0         192.168.19.222   Gi0/1         192.168.60.120  06 0C09 20FB    16
Gi0/0         192.168.12.121   Gi0/1         192.168.60.245  06 0B66 01BB    19
Gi0/0         192.168.14.17    Gi0/1         192.168.60.183  06 0914 1F90     9
Gi0/0         192.168.41.86    Gi0/1         192.168.60.217  06 0B7B 20FB     2
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- en UDP-poorten 5060 en 5061, HTTP-pakketten op TCP-poorten 80 en 8080 en HTTPS-pakketten op TCP-poorten 443 en 8443 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 sip 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 sip
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 www access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8080 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 ! !-
- 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 sip 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 sip 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 www access-list tACL-Policy extended deny tcp any
```

```
192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 ! !-- 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 opdracht **show access-list** gebruiken om het aantal SIP-pakketten op TCP- en UDP-poorten 5060 en 5061, HTTP-pakketten op TCP-poorten 80 en 8080 en HTTPS-pakketten op TCP-poorten 443 en 8443 die zijn gefilterd te 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 toegang-lijst aan ACL-Beleid** volgt:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 17 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
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq www
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq https
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8443
access-list tACL-Policy line 9 extended deny tcp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=30)
access-list tACL-Policy line 10 extended deny tcp any 192.168.60.0 255.255.255.0 eq
```

```
5061 (hitcnt=43)
access-list tACL-Policy line 11 extended deny udp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=70)
access-list tACL-Policy line 12 extended deny udp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=14)
access-list tACL-Policy line 13 extended deny tcp any 192.168.60.0 255.255.255.0 eq
www (hitcnt=45)
access-list tACL-Policy line 14 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=53)
access-list tACL-Policy line 15 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8080 (hitcnt=70)
access-list tACL-Policy line 16 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8443 (hitcnt=61)
access-list tACL-Policy line 17 extended deny tcp any any
```

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

- **30 SIP-**pakketten op **TCP-poort 5060** voor ACE-lijn 9
- **43 SIP-**pakketten op **TCP-poort 5061** voor ACE-lijn 10
- **70 SIP-**pakketten op **UDP-poort 5060** voor ACE-lijn 11
- **14 SIP-**pakketten op **UDP-poort 5061** voor ACE-lijn 12
- **45 HTTP**-pakketten op **TCP-poort 80** voor ACE-lijn 13
- **53 HTTPS-**pakketten op **TCP-poort 443** voor ACE-lijn 14
- **70 HTTP**-pakketten op **TCP-poort 8080** voor ACE-lijn 15
- **61 HTTPS-**pakketten op **TCP-poort 8443** voor ACE-lijn 16

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
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.18/16784
         dst inside:192.168.60.191/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.200/16785
         dst inside:192.168.60.33/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.99/16786
         dst inside:192.168.60.240/5061 by access-group "tACL-Policy"
```

```
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.100/16787
         dst inside:192.168.60.115/5061 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.88/18683
         dst inside:192.168.60.38/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.175/18684
         dst inside:192.168.60.250/5061 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**- 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
  Apr 27 2011 00:03:42: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %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.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

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

- 35846-0 - Cisco CUCM Remote Code-uitvoering
- 35866-0 - Cisco CUCM SIP-kwetsbaarheid
- 35085-0 - Cisco Call Manager SQL-injectie

35846-0 - Cisco CUCM Remote Code-uitvoering

Beginnend met handtekeningsupdate S562 voor sensoren met Cisco IPS versie 6.x en hoger, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 35846/0 (Handtekeningnaam: Cisco CUCM Remote Code Execution). Handtekening 35846/0 is standaard ingeschakeld, activeert een gebeurtenis met *hoge* ernst, heeft een SFR (Signature Fidelity Rating) van 95 en is geconfigureerd met een **waarschuwing voor** standaardgebeurtenissen.

Vuren van handtekening 35846/0 wanneer één pakket wordt verzonden met SIP-poort 5060 gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

35866-0 - Cisco CUCM SIP-kwetsbaarheid

Beginnend met handtekeningsupdate S562 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 35866/0 (Handtekeningnaam: Cisco CUCM SIP Vulnerability). Handtekening 35866/0 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.

Vuren van handtekening 35866/0 wanneer één pakket wordt verzonden met SIP-poort 5060 gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

35085-0 - Cisco Call Manager SQL-injectie

Beginnend met handtekeningsupdate S562 voor sensoren met Cisco IPS versie 6.x en hoger, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 35085/0 (Handtekeningnaam: Cisco Call Manager SQL Injection). Handtekening 35085/0 is standaard ingeschakeld, activeert een gebeurtenis met *hoge* ernst, heeft een SFR (Signature Fidelity Rating) van 85 en is geconfigureerd met een **waarschuwing voor** standaardgebeurtenissen.

Vuren met handtekening 35085/0 bij het detecteren van een SQL-injectieaanval tegen Cisco Call Manager. 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-handtekening 35846/0 (Signature Name: Cisco CUCM Remote Code Execution), IPS-handtekening 35866/0 (Signature Name: Cisco CUCM SIP Vulnerability) en IPS-handtekening 35085/0 (Signature Name: Cisco Call Manager SQL Injection). Nadat de dynamische handtekeningupdate S562 is gedownload, zal het gebruik van sleutelwoord **NR-35846/0** voor IPS-handtekening 35846/0, sleutelwoord **NR-35866/0** voor IPS-handtekening 35866/0 of sleutelwoord **NR-35085/0** voor IPS-handtekening 35085/0 en een vraagtype van **Alle overeenkomende gebeurtenissen** op Cisco Security MARS-applicatie een rapport leveren met een lijst 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 1.1	2011-APRIL-27	Bijgewerkt om informatie voor IPS-handtekeningen en Cisco Security MARS op te nemen.
Revisie 1.0	2011-APRIL-27	Eerste publieke 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

- Presentaties voor Cisco Network Foundation-bescherming
- Een security georiënteerde benadering van IP-adressering
- 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.