Identificatie en beperking van exploitatie van de kwetsbaarheden van Cisco Unified Communications Manager Denial of Service

Identificatie en beperking van exploitatie van de kwetsbaarheden van Cisco Unified Communications Manager Denial of Service

Advies-ID: cisco-amb-20071017-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20071017-cucm

Revisie 1.2

Openbare publicatie 2007 oktober 17 16:00 UTC (GMT)

Inhoud

Cisco Response
Apparaatspecifieke beperking en identificatie
Aanvullende informatie
Revisiegeschiedenis
Cisco-beveiligingsprocedures
Gerelateerde informatie

Cisco Response

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

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in bepaalde releases van Cisco Unified Communications Manager (CUCM), voorheen Cisco Unified CallManager. Deze kwetsbaarheden worden in de volgende subsecties samengevat.

Session Initiation Protocol (SIP) NODIGT UDP Denial of Service uit: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder gebruikersinteractie. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende

DoS-conditie. De aanvalsvector voor exploitatie is via SIP-pakketten met UDP-poort 5060. Een aanvaller kon deze kwetsbaarheid door spoofingaanvallen uitbuiten. Deze kwetsbaarheid is toegewezen CVE-naam CVE-2007-5537.

TFTP-overflow (Central Trivial File Transfer Protocol): deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder gebruikersinteractie. Succesvolle benutting van deze kwetsbaarheid kan willekeurige codeuitvoering toestaan en in een ontkenning van de dienst (Dos) voorwaarde resulteren. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via HTTP-pakketten met TCP-poort 6970. Deze kwetsbaarheid is toegewezen CVE-naam CVE-2007-5538.

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-20071017-cucm.

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor de SIP INVITE UDP-denial of-service en kwetsbaarheden voor gecentraliseerde TFTP-bestandslokalisatieservice. 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.

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 beveiligingsmechanismen filteren en neerzetten, en verifiëren het IP-bronadres van, pakketten die proberen de kwetsbaarheden te exploiteren die in dit document worden beschreven.

Op Cisco IOS-software biedt de juiste implementatie en configuratie van Unicast RPF de meest effectieve bescherming tegen aanvallen waarbij pakketten met IP-adressen van een gespoofde bron worden gebruikt. Unicast RPF moet zo dicht mogelijk bij alle verkeersbronnen worden geïmplementeerd.

De juiste plaatsing en configuratie van IPSG biedt de meest effectieve middelen van bescherming tegen aanvallen met gespoofde bron MAC-adressen.

Effectieve middelen voor explosiepreventie kunnen ook worden geleverd door de Cisco ASA 5500 Series adaptieve security applicatie, Cisco PIX 500 Series security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers met het volgende:

- TACL's
- Unicast RPF

Deze beveiligingsmechanismen filteren en neerzetten, en verifiëren het IP-bronadres van, pakketten die proberen de kwetsbaarheden te exploiteren die in dit document worden beschreven.

Op Cisco ASA, PIX en FWSM biedt de juiste implementatie en configuratie van Unicast RPF de meest effectieve bescherming tegen aanvallen waarbij pakketten met IP-adressen van een gespoofde bron worden gebruikt. Unicast RPF moet zo dicht mogelijk bij alle verkeersbronnen worden geïmplementeerd.

Cisco IOS NetFlow kan zichtbaarheid in deze exploitatiepogingen bieden door gebruik te maken van flowrecords.

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

Effectief gebruik van de gebeurtenisacties van Cisco Inbraakpreventiesysteem (IPS) biedt zichtbaarheid in en bescherming tegen aanvallen die proberen deze kwetsbaarheden te exploiteren.

De applicatie Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan ook zichtbaarheid bieden via vragen en gebeurtenisrapportage.

Risicobeheer

Organisaties moeten hun standaard risicobeoordelings- en risicobeperkingsprocessen 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 Mededelingen en Risico Triage en Prototyping in Informatiebeveiliging Engagements kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

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

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

- Cisco IOS-routers en -Switches
- Cisco IOS NetFlow
- Cisco ASA-, PIX- en FWSM-firewalls
- Cisco-inbraakpreventiesysteem
- Cisco-systeem voor beveiligingsbewaking, analyse en respons

Cisco IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor douanevervoer

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

Het tACL-beleid ontkent onbevoegde SIP-pakketten op UDP-poort 5060 en HTTP-pakketten op TCP-poort 6970 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.1.0/24 is de netwerkIP adresruimte die door de beïnvloede apparaten wordt gebruikt en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

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

```
! !--- Include any explicit permit statements for trusted sources !--- that require access on the vulnerable ports ! access-list 150 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970 ! !--- The following vulnerability-specific access control entries !--- (ACEs) can aid in identification of attacks ! access-list 150 deny udp any 192.168.1.0 0.0.0.255 eq 5060 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 ! !--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance !--- with existing security policies and configurations ! !--- Explicit deny for all other IP traffic ! access-list 150 deny ip any any ! !--- Apply tACL to 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*.

Unicast doorsturen van omgekeerde paden

De SIP INVITE UDP-ontkenning van kwetsbaarheid voor services kan worden gebruikt door gespoofde IP-pakketten. De juiste implementatie en configuratie van Unicast Reverse Path Forwarding (Unicast RPF) kan beschermingsmechanismen bieden voor spoofing in verband met de SIP INVITE UDP-ontkenning van servicekwetsbaarheid.

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 100 procent spoofing bescherming te bieden, omdat spoofed-pakketten het netwerk kunnen binnenkomen via een Unicast RPF-enabled interface als er een geschikte retourroute naar het bron-IP-adres bestaat. Beheerders dienen ervoor te zorgen dat de juiste Unicast RPF-modus (los of strikt) wordt geconfigureerd tijdens de implementatie van deze functie, omdat legitiem verkeer dat via het netwerk wordt verzonden, 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 is beschikbaar 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. De juiste implementatie en configuratie van IPSG gekoppeld aan strikte modus Unicast RPF kan de meest effectieve manier van spoofing bescherming bieden om de SIP INVITE UDP denial of service kwetsbaarheid te helpen verminderen.

Aanvullende informatie over de implementatie en configuratie van IPSG is beschikbaar in Configureren van 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 UDP-poort 5060 en HTTP-pakketten op TCP-poort 6970 identificeren die zijn gefilterd. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten 150** volgt:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970
    30 deny udp any 192.168.1.0 0.0.0.255 eq 5060 (12 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 (26 matches)
    50 deny ip any any
router#
```

In het voorafgaande voorbeeld heeft toegangslijst 150 12 SIP-pakketten op UDP-poort 5060 laten vallen voor ACE-sequentie-id 30 en **26 HTTP-**pakketten op **TCP**-poort **6970** voor ACE-sequentie-id 40.

Identificatie: Vastlegging toegangslijst

De optie **log** of **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.

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. De opdracht **interval-***in-ms* **voor** *vastlegging van* **IP-toegangslijst** kan de effecten van processwitching beperken die worden veroorzaakt door ACL-vastlegging. De **logsnelheid-limiet** *rate-per-seconde* [**behalve** *loglevel*] opdracht beperkt het effect van loggeneratie en transmissie.

Voor extra informatie over de configuratie en het gebruik van ACL-vastlegging raadpleegt u het Witboek 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 interface van de show gebruiken, **cef drop tonen**, **cef interface** *type sleuf/poort* **intern tonen**, en **ip traffic** opdrachten tonen om het aantal pakketten te identificeren dat Unicast RPF is gedaald.

Opmerking: de *opdracht* **show** | **begin met** *regexp* en **toon** *opdracht* | **omvat** *regexp* commando modifiers worden gebruikt in de volgende voorbeelden om de hoeveelheid output te minimaliseren die beheerders moeten parseren om de gewenste informatie te bekijken. Er is aanvullende informatie over opdrachtwijzigingen beschikbaar in de secties "show commando" van de Opdrachtreferentie voor Cisco IOS Configuration Fundamentals.

Opmerking: Het **show cef interface** *type sleuf/poort* **interne** opdracht 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
    !--- CLI Output Truncated
   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
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route    No_adj
RP             0           0           0           3         0
router#
```

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
      --      CLI Output Truncated       --
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow self-ping
router#
```

```
router#show ip traffic

IP statistics:
  Rcvd:  68051015 total, 2397325 local destination
         43999 format errors, 0 checksum errors, 33 bad hop count
```

```
        2 unknown protocol, 929 not a gateway
        21 security failures, 190123 bad options, 542768 with options
  Opts:  352227 end, 452 nop, 36 basic security, 1 loose source route
        45 timestamp, 59 extended security, 41 record route
        53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
        361634 other
  Frags: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
        0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 64666 received, 0 sent
  Mcast: 1589885 received, 2405454 sent
  Sent:  3001564 generated, 65359134 forwarded

  Drop:  4256 encapsulation failed, 0 unresolved, 0 no adjacency
        18 no route, 18 unicast RPF, 0 forced drop
        0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
    !--- CLI Output Truncated router#
```

In de bovenstaande voorbeelden is Unicast RPF **18 IP-pakketten** gevallen die wereldwijd op alle interfaces met Unicast RPF zijn ontvangen, geconfigureerd vanwege het onvermogen om het bronadres van de IP-pakketten te verifiëren in de Cisco Express Forwarding Forwarding Information Base.

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 pogingen kunnen zijn om de kwetsbaarheden te exploiteren die in dit document worden beschreven. De beheerders zouden stromen moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.

```
router#show ip cache flow

IP packet size distribution (1103375 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .004 .434 .081 .017 .011 .033 .001 .010 .001 .000 .009 .000 .001 .001 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .002 .380 .002 .004 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  12 active, 65524 inactive, 54766 added
  3098504 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
  IP Sub Flow Cache, 402120 bytes
  24 active, 16360 inactive, 109532 added, 54766 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         869      0.0        38    41      0.1      20.6      43.2
TCP-FTP             31      0.0        16    59      0.0       6.7      28.0
TCP-WWW           2996      0.0        12   231      0.1       8.2      11.4
TCP-other        24997      0.0        38   288      3.3      25.5      21.1
UDP-DNS            361      0.0         2    49      0.0       0.9      60.4
```

```
UDP-NTP          13982      0.0         1    76      0.0       0.8      60.5
UDP-other        10136      0.0         3   159      0.1      25.3      48.6
ICMP               556      0.0         7    68      0.0      51.4      39.6
Total:           53928      0.1        20   270      3.7      18.1      36.8

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64  Gi0/1         192.168.1.21    11 13C4 13C4  1458
Gi0/0         192.16820.67    Gi0/1         192.168.150.60  06 0707 0016    80
Gi0/0         192.168.208.63  Gi0/1         192.168.1.21    06 84F2 1B3A     4
Gi0/0         192.168.14.132  Gi0/1         192.168.150.60  06 1A29 90AB     2
Gi0/0         192.168.115.113 Gi0/1         192.168.128.21  06 09BD 0017     2
Gi0/0         192.168.115.113 Local         192.168.128.20  06 0981 0017    31
Gi0/0         192.168.115.113 Gi0/1         192.168.130.41  06 0B83 01BB    30
Gi0/0         192.168.226.1   Gi0/1         192.168.206.5   11 007B 007B     1
Gi0/0         192.168.226.1   Local         192.168.128.20  11 007B 007B     1
Gi0/0         192.168.226.1   Gi0/1         192.168.128.21  11 007B 007B     1
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor SIP-pakketten op UDP-poort 5060 **(hexawaarde 13C4)** en HTTP-pakketten op TCP-poort 6970 **(hexawaarde 1B3A)**. De UDP-pakketten in deze stromen kunnen worden gespookt en kunnen wijzen op een poging om de in dit document beschreven kwetsbaarheden te exploiteren. De beheerders zouden deze stromen bij basislijngebruik voor SIP-pakketten op UDP-poort 5060 en op TCP-poort 6970 moeten vergelijken en ook de stromen moeten onderzoeken om te bepalen of ze afkomstig zijn van onbetrouwbare hosts of netwerken.

Als u alleen de verkeersstromen voor SIP-pakketten op UDP-poort 5060 **(hexadecimale waarde 13C4)** wilt weergeven, **toont** de opdracht de **IP-cachestroom | neem ook SrcIf|_11_.*13C4** zal de verwante verslagen NetFlow zoals hier getoond tonen:

```
router#show ip cache flow | include SrcIf|_11_.*13C4
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64   Gi0/1 192.168.1.21    11 13C4 13C4  1458
router#
```

Als u alleen de verkeersstromen voor TCP-poort 6970 **(hexadecimale waarde 1B3A)** wilt weergeven, **toont** de opdracht de **IP-cachestroom | omvat ook SrcIf|_06_.*1B3A** zal de verwante verslagen NetFlow zoals hier getoond tonen:

```
router#show ip cache flow | include SrcIf|_06_.*1B3A
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.63   Gi0/1 192.168.1.21    06 84F2 1B3A     4
router#
```

Cisco ASA-, PIX- en FWSM-firewalls

Beperking: toegangscontrolelijsten voor douanevervoer

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

Het tACL-beleid ontkent onbevoegde SIP-pakketten op UDP-poort 5060 en HTTP-pakketten op

TCP-poort 6970 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.1.0/24 is de netwerkIP adresruimte die door de beïnvloede apparaten wordt gebruikt en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

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

```
! !--- Include any explicit permit statements for trusted sources !--- that require
access on the vulnerable ports ! access-list Transit-ACL-Policy extended permit udp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 6970 ! !--- The
following vulnerability-specific access control entries !--- (ACEs) can aid in
identification of attacks ! access-list Transit-ACL-Policy extended deny udp any
192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy extended deny tcp
any 192.168.1.0 255.255.255.0 eq 6970 ! !--- Permit/deny all other Layer 3 and Layer
4 traffic in accordance !--- with existing security policies and configurations ! !--
- Explicit deny for all other IP traffic ! access-list Transit-ACL-Policy extended
deny ip any any ! !--- Apply tACL to interfaces in the ingress direction ! access-
group Transit-ACL-Policy in interface outside
```

Beperking: bescherming tegen spoofing met Unicast Reverse Path Forwarding

De SIP INVITE UDP-ontkenning van kwetsbaarheid voor services kan worden gebruikt door gespoofde IP-pakketten. De juiste implementatie en configuratie van Unicast Reverse Path Forwarding (Unicast RPF) kan beschermingsmechanismen bieden voor spoofing in verband met de SIP INVITE UDP-ontkenning van servicekwetsbaarheid.

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 100 procent spoofing bescherming te bieden, omdat spoofed-pakketten het netwerk kunnen binnenkomen via een Unicast RPF-enabled interface 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 ondersteunend Layer 3 interfaces kunnen worden toegelaten.

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 UDP-poort 5060 en HTTP-pakketten op TCP-poort 6970 te identificeren die zijn gefilterd. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont toegang-lijst Transit-ACL-Policy** volgt:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1
```

```
192.168.1.0 255.255.255.0 eq sip
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 6970
access-list Transit-ACL-Policy line 3 extended deny udp any 192.168.1.0 255.255.255.0
eq sip (hitcnt=4378)
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255.255.0
eq 6970
access-list Transit-ACL-Policy line 5 extended deny ip any any
firewall#
```

In het voorafgaande voorbeeld heeft de toegangslijst *Transit-ACL-Policy* **4378** SIP-pakketten op UDP-poort **5060** laten vallen die van een onbetrouwbare host of een onbetrouwbaar netwerk zijn ontvangen. Daarnaast kan syslog-bericht *106023* waardevolle informatie leveren, waaronder het IP-adres van de bron en de bestemming, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket.

Identificatie: berichten in Firewall Access-list Syslog

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 is beschikbaar in het systeemlogbericht van Cisco Security Appliance - 106023.

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

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

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

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-4-106023: Deny udp src outside:192.168.2.18/5210 dst
   inside:192.168.1.191/5060 by access-group "Transit-ACL-Policy"
Sep 20 2007 10:07:01: %ASA-4-106023: Deny tcp src outside:192.168.3.200/3521 dst
   inside:192.168.1.33/6970 by access-group "Transit-ACL-Policy"
firewall#
```

In het voorafgaande voorbeeld heeft de toegangslijst *Transit-ACL-Policy* **4378** SIP-pakketten op UDP-poort **5060** laten vallen die van een onbetrouwbare host of een onbetrouwbaar netwerk zijn ontvangen. Daarnaast kan syslog-bericht *106023* waardevolle informatie leveren, waaronder het IP-adres van de bron en de bestemming, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket.

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

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 is beschikbaar in het systeemlogbericht van Cisco Security Appliance - 106021.

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

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

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

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny TCP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
firewall#
```

De opdracht **Snel** starten tonen kan ook het aantal pakketten identificeren dat Unicast RPF heeft laten vallen, zoals in het volgende voorbeeld:

```
firewall#show asp drop

Frame drop:
  Reverse-path verify failed                          11
  Flow is denied by configured rule                  855
  Expired flow                                         1
  Interface is down                                    2

Flow drop:

firewall#
```

In het voorafgaande voorbeeld heeft Unicast RPF **11 IP-pakketten** laten vallen die zijn ontvangen op interfaces met Unicast RPF geconfigureerd.

Voor extra informatie over de configuratie en het gebruik van Unicast PDF, raadpleegt u de Cisco Security Appliance Command Reference voor weergave van de asp-drop.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

Beheerders kunnen de Cisco Inbraakpreventiesysteem (IPS) applicaties en servicesmodules 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:

- 5912/2010 - CUCM SIP NODIGT UDP-serviceweigering uit
- 5910/2010 - CUCM gecentraliseerde TFTP-bestandslocator voor servicebufferoverloop

5912/00 - CUCM SIP NODIGT UDP Denial of Service uit.

Beginnend met handtekeningsupdate S307 voor sensoren met Cisco IPS versie 6.x of 5.x, kunnen de kwetsbaarheden die in dit document worden beschreven worden gedetecteerd door handtekening 6912/0 (Handtekeningnaam: CUCM Gecentraliseerde TFTP File Locator Service Buffer Overflow. Signature 5912/0 is standaard ingeschakeld, activeert een *Medium* Severity event, heeft een Signature Fidelity Rating (SFR) van 80 en is geconfigureerd met een default event actie van **Produce Alert**. Vuren van 5912/0 wanneer meerdere pakketten die met UDP-poort 5060 zijn verzonden, worden gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk gebruik van de in dit document beschreven kwetsbaarheden.

5910/1900 - CUCM gecentraliseerde TFTP File Locator Service Buffer Overflow.

Beginnend met handtekeningsupdate S307 voor sensoren met Cisco IPS versie 6.x of 5.x, kunnen de kwetsbaarheden die in dit document worden beschreven worden gedetecteerd door handtekening 5910/0 (Handtekeningnaam: CUCM Gecentraliseerde TFTP File Locator Service Buffer Overflow). Signature 5910/0 is standaard ingeschakeld, activeert een *Medium* Severity event, heeft een SFR van 75 en is geconfigureerd met een default event action van **Produce Alert** . Vuren van handtekening 5910/0 wanneer meerdere pakketten verzonden met TCP-poort 6970 worden gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk gebruik van de in dit document beschreven 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.

De oprichting van de handdruk met drie richtingen van TCP wordt vereist om deze kwetsbaarheid te exploiteren, die de mogelijkheid van succesvolle aanvallen met behulp van gespoofde IP-adressen evenals valse positieve gebeurtenissen voor handtekening 5910/0 vermindert.

Omdat op UDP gebaseerde exploits eenvoudig kunnen worden gespoofd, kan een aanval die gespoofde adressen bevat ervoor zorgen dat een geconfigureerde gebeurtenisactie per ongeluk verkeer van vertrouwde bronnen ontkent. Gebeurtenisacties die blokkering via ACL's of de shun-opdracht uitvoeren, worden doorgaans geconfigureerd op sensoren die in promiscuous mode worden ingezet.

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-sensoren die in de modus voor inline bescherming worden geïmplementeerd, biedt bedreigingspreventie tegen een aanval die probeert deze kwetsbaarheden te exploiteren. De preventie van de bedreiging wordt bereikt door een standaardopheffing die een gebeurtenis actie van **Deny Connection Inline** uitvoert en **Waarschuwing** voor teweeggebrachte handtekeningen **produceert** met een *riskRatingValue* groter dan 90. Aanvullende informatie over de risicoclassificatie en de berekening van de waarde ervan

is beschikbaar in de uitleg van Cisco IPS Risk Rating.

Cisco IPS 5.x-sensoren die in inline-beschermingsmodus worden geïmplementeerd, moeten per handtekening een gebeurtenisactie hebben geconfigureerd. Alternatief, kunnen de beheerders een opheffing vormen die een gebeurtenisactie voor om het even welke handtekeningen kan uitvoeren die worden teweeggebracht en als hoog-risico bedreiging berekend. Het gebruik van de **Deny Connection Inline** and **Produce Alert** Event-actie op sensoren die in inline-beschermingsmodus worden ingezet, biedt de meest effectieve exploit-preventie.

Identificatie: gebeurtenissen voor IPS-handtekeningen

5912/00 - CUCM SIP NODIGT UDP Denial of Service uit.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278931859 severity=medium vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:14:21 2007/10/17 12:14:21 CDT
  signature: description=CUCM SIP INVITE UDP Denial of Service id=5912 version=S307
    subsigId: 0
    sigDetails: CUCM SIP INVITE UDP Denial of Service
    marsCategory: DoS/Network/UDP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.64
      port: 5060
    target:
      addr: locality=OUT 192.168.132.44
      port: 5060
      os: idSource=learned relevance=relevant type=linux
   triggerPacket:
 !--- Packet details removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 60 threatRatingValue: 60 interface: ge0_0 protocol: udp
```

5910/1900 - CUCM gecentraliseerde TFTP File Locator Service Buffer Overflow.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278930978 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:00:57 2007/10/17 12:00:57 CDT
  signature: description=CUCM Centralized TFTP File Locator Service Buffer Overflow
id=5910 version=S307
    subsigId: 0
    sigDetails: Buffer overflow in TFTP over HTTP
    marsCategory: Penetrate/BufferOverflow/Web
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
      port: 32806
```

```
    target:
      addr: locality=OUT 192.168.132.44
      port: 6970
      os: idSource=learned relevance=relevant type=linux
    context:
      fromAttacker:
!--- Packet Details Removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium watchlist=25 81 threatRatingValue: 81 interface: ge0_0
protocol: tcp
```

[Cisco-systeem voor beveiligingsbewaking, analyse en respons]

Identificatie: Type en trefwoord voor Cisco Security Monitoring, Analysis en Response System Query

Het apparaat Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan vragen stellen over gebeurtenissen voor de CUCM-denial of service-kwetsbaarheden met behulp van een query-type en een trefwoord. Gebruik van een trefwoord van NR-5912/0 voor IPS-handtekening **5912/0**, die de SIP INVITE UDP-denial of service kwetsbaarheid kan detecteren; trefwoord van **NR-5910/0** voor IPS-handtekening **5910/0**, die de gecentraliseerde TFTP-overflow kwetsbaarheid van de bestandslocatiedienst kan detecteren; en een zoektype van **Alle overeenkomende onbewerkte berichten** op het Cisco Security MARS-apparaat zal een rapport leveren met de gebeurtenissen die zijn gemaakt door IPS2591 0/0 of 5910/0.

De volgende schermopname toont de waarden die worden gebruikt om te zoeken naar gebeurtenissen die zijn gemaakt met IPS-handtekening 5912/0 (Handtekeningnaam: CUCM SIP INVITE UDP Denial of Service) of IPS-handtekening 5910/0 (Handtekeningnaam: CUCM Gecentraliseerde TFTP File Locator Service Buffer Overflow).

Het volgende schermschot toont de vraagresultaten voor **NR-5912/0 of NR-5910/0** die door het apparaat van Cisco Security MARS worden gecreëerd die een vraagtype en een vraag van het sleutelwoord regex gebruiken.

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 1.2	2007-22 oktober	Toegewezen CVE-namen opnemen
Revisie 1.1	2007-okt-17	Omvat IPS handtekeningspak S307 informatie
Revisie 1.0	2007-okt-17	Eerste openbare publicatie

Cisco-beveiligingsprocedures

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

Gerelateerde informatie

- Cisco-bulletins voor toegepaste beperking
- Uw kern beveiligen: toegangscontrolelijsten voor infrastructuurbescherming
- Transit Access Control Lists: filtering aan uw rand
- Vastlegging toegangscontrolelijst begrijpen
- Doorsturen van unicast-omgekeerde paden
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- Cisco Firewallproducten - startpagina op Cisco.com
- Unicast omgekeerde pad doorsturen in losse modus
- Gemeenschappelijke kwetsbaarheden en blootstellingen (CVE)
- Cisco 6.x inbraakpreventiesysteem
- Cisco IPS-risicoclassificatie toegelicht
- Cisco IPS 6.x downloads voor handtekeningen
- Cisco IPS-handtekeningen per release versie (alleen geregistreerde klanten)
- Cisco IPS-handtekeningen via handtekenings-ID (alleen geregistreerde klanten)
- Cisco-systeem voor beveiligingsbewaking, analyse en respons

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.