# Identifizieren und Eindämmen der Ausnutzung der Denial-of-Service-Sicherheitslücken in Cisco Unified Communications Manager

# Identifizieren und Eindämmen der Ausnutzung der Denial-of-Service-Sicherheitslücken in Cisco Unified Communications Manager

**Beratungs-ID: cisco-amb-20071017-cucm**

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

## Version 1.2

**Zur öffentlichen Veröffentlichung 2007 17. Oktober 16:00 UTC (GMT)**

---

## Inhalt



---

## Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zu den PSIRT Security Advisory *Cisco Unified Communications Manager Denial of Service-Schwachstellen* und bietet Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

### Merkmale der Schwachstelle

Bestimmte Versionen von Cisco Unified Communications Manager (CUCM), früher Cisco Unified CallManager, weisen mehrere Schwachstellen auf. Diese Schwachstellen werden in den folgenden Unterabschnitten zusammengefasst.

**Session Initiation Protocol (SIP) INVITE UDP Denial of Service:** Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff aus der Ferne ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem

anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung wird durch SIP-Pakete über den UDP-Port 5060 generiert. Ein Angreifer könnte diese Schwachstelle durch Spoofing-Angriffe ausnutzen. Dieser Verwundbarkeit wurde der CVE-Name CVE-2007-5537 zugewiesen.

**Centralized Trivial File Transfer Protocol (TFTP) File Locator Service Overflow:** Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff aus der Ferne ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen und zu einer Denial of Service (DoS)-Bedingung führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung wird über HTTP-Pakete mit dem TCP-Port 6970 generiert. Dieser Verwundbarkeit wurde der CVE-Name CVE-2007-5538 zugewiesen.

Informationen zu anfälliger, nicht betroffener und fest installierter Software finden Sie in der PSIRT-Sicherheitsberatung, die unter folgendem Link verfügbar ist: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071017-cucm.

## Überblick über die Risikominderungstechnik

Cisco Geräte bieten mehrere Gegenmaßnahmen gegen die Diensteverweigerung durch SIP INVITE UDP und die Überlaufschwachstellen des Centralized TFTP File Locator Service. Den Administratoren wird empfohlen, diese Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs im Netzwerk zu betrachten.

Die Cisco IOS Software bietet mithilfe der folgenden Methoden einen effektiven Schutz vor Exploits:

- Transit-Zugriffskontrolllisten (tACLs)
- Unicast Reverse Path Forwarding (Unicast-RPF)
- IP Source Guard (IPSG)

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, die in diesem Dokument beschriebenen Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.

Die Cisco IOS Software bietet durch die richtige Bereitstellung und Konfiguration von Unicast RPF den effektivsten Schutz gegen Angriffe, die Pakete mit gefälschten Quell-IP-Adressen verwenden. Unicast-RPF sollte so nahe wie möglich an allen Datenverkehrsquellen bereitgestellt werden.

Die ordnungsgemäße Bereitstellung und Konfiguration von IPSG bietet mit gefälschten Quell-MAC-Adressen den effektivsten Schutz vor Angriffen.

Die Cisco Adaptive Security Appliance der Serie ASA 5500, die Cisco Security Appliance der Serie PIX 500 und das Firewall Services Module (FWSM) für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 bieten ebenfalls eine effektive Exploit-Abwehr. Dazu werden folgende Funktionen verwendet:

- tACL
- Unicast RPF

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, die in diesem Dokument beschriebenen Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.

Auf Cisco ASA, PIX und FWSM bietet die ordnungsgemäße Bereitstellung und Konfiguration von

Unicast RPF den effektivsten Schutz gegen Angriffe, die Pakete mit gefälschten Quell-IP-Adressen verwenden. Unicast-RPF sollte so nahe wie möglich an allen Datenverkehrsquellen bereitgestellt werden.

Cisco IOS NetFlow kann mithilfe von Flow Records einen Überblick über diese Exploit-Versuche geben.

Cisco IOS Software, Cisco ASA, Cisco PIX Security Appliances und FWSM-Firewalls bieten Transparenz durch Syslog-Meldungen und die Zählerwerte, die in der Ausgabe der **show-**Befehle angezeigt werden.

Die effektive Nutzung von Cisco Intrusion Prevention System (IPS)-Ereignisaktionen bietet Transparenz und Schutz vor Angriffen, die diese Schwachstellen ausnutzen.

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance bietet ebenfalls Transparenz durch Abfragen und Ereignisberichte.

### Risikomanagement

Unternehmen sollten ihre standardmäßigen Risikobewertungs- und Minderungsprozesse befolgen, um die potenziellen Auswirkungen dieser Schwachstellen zu ermitteln. Triage bezieht sich auf das Sortieren von Projekten und die Priorisierung von Bemühungen, die am wahrscheinlichsten erfolgreich sein werden. Cisco hat Dokumente bereitgestellt, die Unternehmen bei der Entwicklung einer risikobasierten Triage-Funktion für ihre Informationssicherheitsteams unterstützen. Risikoanalyse für Sicherheitslücken Ankündigungen und Risikoanalyse und Prototyping in Information Security Engagements können Unternehmen dabei unterstützen, wiederholbare Sicherheitsbewertungs- und Reaktionsprozesse zu entwickeln.

## Gerätespezifische Eindämmung und Identifizierung

**Vorsicht:** Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Spezifische Informationen zur Risikominderung und Identifizierung sind für diese Geräte verfügbar:

- Cisco IOS-Router und -Switches
- Cisco IOS-NetFlow
- Cisco ASA, PIX und FWSM-Firewalls
- Cisco Intrusion Prevention System
- Cisco Security Monitoring, Analysis and Response System

### Cisco IOS-Router und -Switches

#### Eindämmung: Transit-Zugriffskontrolllisten

Um das Netzwerk vor Datenverkehr zu schützen, der an Eingangs-Access Points in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Partner- und Lieferantenverbindungspunkte oder VPN-Verbindungspunkte, sollten Administratoren Transit-Zugriffskontrolllisten (tACLs) bereitstellen, um die Richtlinien durchzusetzen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr an den Eingangs-Access Points in das Netzwerk eindringt, oder indem sie autorisiertem Datenverkehr gestatten, das Netzwerk gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen zu passieren.

Die tACL-Richtlinie verweigert nicht autorisierte SIP-Pakete auf dem UDP-Port 5060 und HTTP-Pakete auf dem TCP-Port 6970, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.1.0/24 der von den betroffenen Geräten verwendete IP-Adressraum des Netzwerks, und der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie unter 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 !
```

Beachten Sie, dass das Filtern mit einer Schnittstellenzugriffsliste die Übertragung von nicht erreichbaren ICMP-Nachrichten zurück an die Quelle des gefilterten Datenverkehrs auslöst. Das Generieren dieser Nachrichten könnte den unerwünschten Effekt einer erhöhten CPU-Auslastung auf dem Gerät haben. In Cisco IOS-Software ist nicht-erreichbare Generation ICMP auf ein Paket alle 500 Millisekunden standardmäßig begrenzt. Die Erzeugung von nicht erreichbaren ICMP-Nachrichten kann mit dem Schnittstellenkonfigurationsbefehl **no ip unreachables** deaktiviert werden. Die Durchsatzbegrenzung "ICMP unreachable" kann mithilfe des globalen Konfigurationsbefehls **ip icmp rate-limit unreachable** *interval-in-ms* vom Standardwert geändert werden.

### Unicast Reverse Path Forwarding

Die Diensteverweigerungsschwachstelle SIP INVITE UDP kann durch gefälschte IP-Pakete ausgenutzt werden. Die ordnungsgemäße Bereitstellung und Konfiguration von Unicast Reverse Path Forwarding (Unicast RPF) kann Schutzmechanismen für Spoofing im Zusammenhang mit der Diensteverweigerungsschwachstelle SIP INVITE UDP bereitstellen.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen hundertprozentigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. Administratoren sollten sicherstellen, dass während der Bereitstellung dieser Funktion der entsprechende Unicast RPF-

Modus (flexibel oder strikt) konfiguriert wird, da legitimer Datenverkehr, der das Netzwerk durchquert, verworfen werden kann. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützenden Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen finden Sie im Funktionsleitfaden zur Unicast Reverse Path Forwarding Loose Mode.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie im Whitepaper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

### IP-Quellschutz

IP Source Guard (IPSG) ist eine Sicherheitsfunktion, die den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen beschränkt, indem Pakete auf Basis der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierter IP-Source-Bindings gefiltert werden. Administratoren können IPSG verwenden, um Angriffe eines Angreifers zu verhindern, der versucht, Pakete durch Fälschung der Quell-IP-Adresse und/oder der MAC-Adresse zu fälschen. Die ordnungsgemäße Bereitstellung und Konfiguration von IPSG in Verbindung mit dem Unicast-RPF im strikten Modus bietet den wirksamsten Spoofing-Schutz, um eine Diensteverweigerung durch SIP INVITE UDP zu verhindern.

Weitere Informationen zur Bereitstellung und Konfiguration von IPSG finden Sie unter Konfigurieren der DHCP-Funktionen und von IP Source Guard.

### Identifizierung: Transit-Zugriffskontrolllisten

Nachdem der Administrator die tACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der SIP-Pakete auf dem UDP-Port 5060 und der HTTP-Pakete auf dem TCP-Port 6970, die gefiltert wurden. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show ip access-lists 150**:

```
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#
```

Im vorherigen Beispiel hat die Zugriffsliste 150 12 SIP-Pakete auf dem UDP-Port 5060 für die ACE-Sequenz-ID 30 verworfen und **26 HTTP-**Pakete auf dem **TCP-**Port **6970** für die ACE-Sequenz-ID 40.

### Identifizierung: Protokollierung der Zugriffsliste

Die Option **log** oder **log-input** access control list (ACL) bewirkt, dass Pakete protokolliert werden, die bestimmten ACEs entsprechen. Die Option **log-input** ermöglicht die Protokollierung der Eingangsschnittstelle zusätzlich zu den IP-Adressen und -Ports für die Paketquelle und das Ziel.

**Achtung: Die** Protokollierung von Zugriffskontrolllisten kann sehr CPU-intensiv sein und muss mit äußerster Vorsicht verwendet werden. Faktoren, die die Auswirkungen der ACL-Protokollierung

auf die CPU verstärken, sind die Protokollgenerierung, die Protokollübertragung und das Prozess-Switching, um Pakete weiterzuleiten, die mit protokollfähigen ACEs übereinstimmen.

Die CPU-Auswirkungen der ACL-Protokollierung können mithilfe optimierter ACL-Protokollierung in der Hardware auf den Cisco Catalyst Switches der Serie 6500 und den Cisco Routern der Serie 7600 mit der Supervisor Engine 720 oder der Supervisor Engine 32 berücksichtigt werden. Der Befehl **ip access-list logging interval** *interval-in-ms* kann die Auswirkungen des durch die ACL-Protokollierung induzierten Prozesswechsels begrenzen. Der Befehl **logging rate-limit** *rate-per-second* [**except** *loglevel*] begrenzt die Auswirkungen der Protokollgenerierung und -übertragung.

Weitere Informationen zur Konfiguration und Verwendung der ACL-Protokollierung finden Sie im Whitepaper Understanding Access Control List Logging Applied Intelligence.

### Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Wenn Unicast RPF ordnungsgemäß in der gesamten Netzwerkinfrastruktur bereitgestellt und konfiguriert ist, können Administratoren die Befehle show ip interface, **show cef drop**, **show cef interface** *type slot/port* **internal** und **show ip traffic**-Befehle verwenden,um die Anzahl der Pakete zu identifizieren, die von Unicast RPF verworfen wurden.

**Hinweis:** Der *Befehl* **show** | **begin** *regexp* and **show** *command* | **include** *regexp*-Befehlsmodifizierer werden in den folgenden Beispielen verwendet, um die Ausgabe zu minimieren, die Administratoren analysieren müssen, um die gewünschten Informationen anzuzeigen. Weitere Informationen zu Befehlsmodifizierern finden Sie in der Befehlsreferenz zu den Cisco IOS-Konfigurationsgrundlagen im Abschnitt "show command" (Befehl anzeigen).

**Hinweis:** Der Befehl **show cef interface** *type slot/port* **internal** ist ein ausgeblendeter Befehl, der vollständig in die Befehlszeilenschnittstelle eingegeben werden muss. Die Befehlsvervollständigung steht dafür nicht zur Verfügung.

```
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 den vorherigen Beispielen hat Unicast RPF **18** global empfangene **IP-Pakete** an allen Schnittstellen mit konfiguriertem Unicast RPF verworfen, da die Quelladresse der IP-Pakete in der Cisco Express Forwarding Forwarding Information Base nicht verifiziert werden konnte.

## Cisco IOS-NetFlow

### Identifizierung: Identifikation des Datenverkehrsflusses mithilfe von NetFlow-Datensätzen

Administratoren können Cisco IOS NetFlow auf Cisco IOS-Routern und -Switches konfigurieren, um Datenverkehrsflüsse zu identifizieren, bei denen versucht werden kann, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Administratoren sollten Datenströme untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen, oder ob es sich um legitime Datenströme handelt.

```
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#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für SIP-Pakete auf UDP-Port 5060 (**Hex-Wert 13C4)** und HTTP-Pakete auf TCP-Port 6970 (**Hex-Wert 1B3A)**. Die UDP-Pakete in diesen Flows können gefälscht werden und einen Versuch darstellen, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Administratoren sollten diese Datenflüsse mit der Basisauslastung für SIP-Pakete auf dem UDP-Port 5060 und dem TCP-Port 6970 vergleichen und sie untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.

Um nur die Datenverkehrsflüsse für SIP-Pakete auf dem UDP-Port 5060 (**Hexadezimalwert 13C4) anzuzeigen,** muss der Befehl **show ip cache flow (IP-Cache-Fluss) | include SrcIf|_11_.*13C4** zeigt die zugehörigen NetFlow-Datensätze wie folgt an:

```
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#
```

Um nur die Datenverkehrsflüsse für TCP-Port 6970 (**Hexadezimalwert 1B3A) anzuzeigen**, wird der Befehl **show ip cache flow (IP-Cachefluss anzeigen) | include SrcIf|_06_.*1B3A** zeigt die zugehörigen NetFlow-Datensätze wie folgt an:

```
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 und FWSM-Firewalls

### Eindämmung: Transit-Zugriffskontrolllisten

Um das Netzwerk vor Datenverkehr zu schützen, der an Eingangs-Access Points in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Verbindungspunkte von Partnern und Lieferanten oder VPN-Verbindungspunkte, sollten Administratoren tACLs bereitstellen, um die Richtlinien durchzusetzen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr an den Eingangs-Access Points in das Netzwerk eindringt, oder indem sie autorisiertem Datenverkehr gestatten, das Netzwerk gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen zu passieren.

Die tACL-Richtlinie verweigert nicht autorisierte SIP-Pakete auf dem UDP-Port 5060 und HTTP-

Pakete auf dem TCP-Port 6970, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.1.0/24 der von den betroffenen Geräten verwendete IP-Adressraum des Netzwerks, und der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie unter 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
```

### Eindämmung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die Diensteverweigerungsschwachstelle SIP INVITE UDP kann durch gefälschte IP-Pakete ausgenutzt werden. Die ordnungsgemäße Bereitstellung und Konfiguration von Unicast Reverse Path Forwarding (Unicast RPF) kann Schutzmechanismen für Spoofing im Zusammenhang mit der Diensteverweigerungsschwachstelle SIP INVITE UDP bereitstellen.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen hundertprozentigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützenden Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie in der Cisco Security Appliance Command Reference for **ip verify reverse path** und im Whitepaper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

### Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der SIP-Pakete auf dem UDP-Port 5060 und der HTTP-Pakete auf dem TCP-Port 6970 identifizieren, die gefiltert wurden. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show access-list Transit-ACL-Policy**:

```
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#
```

Im vorherigen Beispiel hat die Zugriffsliste "*Transit-ACL-Policy*" **4378** SIP-Pakete auf dem UDP-Port **5060** verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden. Darüber hinaus kann die Syslog-Meldung *106023* nützliche Informationen bereitstellen, z. B. die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Port-Nummern und das IP-Protokoll für das abgelehnte Paket.

### Identifizierung: Firewall Access-Liste Syslog-Meldungen

Die Firewall-Syslog-Meldung *106023* wird für Pakete generiert, die von einem Zugriffskontrolleintrag (Access Control Entry, ACE) abgelehnt wurden, für die kein **log-**Schlüsselwort vorhanden ist. Weitere Informationen zu dieser Syslog-Meldung finden Sie unter Cisco Security Appliance System Log Message - 106023.

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 oder die Cisco Security Appliance der Serie PIX 500 finden Sie unter Configuring Logging (Konfigurieren der Protokollierung) auf der Cisco Security Appliance. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie unter Configuring Monitoring and Logging on the Cisco FWSM.

Im folgenden Beispiel **zeigt** die **Protokollierung | grep** *regex* extrahiert Syslog-Meldungen aus dem Protokollierungspuffer der Firewall. Diese Meldungen enthalten zusätzliche Informationen zu abgelehnten Paketen, die auf Versuche hinweisen könnten, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Es ist möglich, verschiedene reguläre Ausdrücke mit dem **grep-**Schlüsselwort zu verwenden, um nach bestimmten Daten in den protokollierten Nachrichten zu suchen.

Weitere Informationen zur Syntax regulärer Ausdrücke finden Sie unter Verwenden der Befehlszeilenschnittstelle.

```
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#
```

Im vorherigen Beispiel hat die Zugriffsliste "*Transit-ACL-Policy*" **4378** SIP-Pakete auf dem UDP-Port **5060** verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden. Darüber hinaus kann die Syslog-Meldung *106023* nützliche Informationen bereitstellen, z. B. die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Port-Nummern und das IP-Protokoll für das abgelehnte Paket.

Weitere Informationen zu Syslog-Meldungen für ASA- und PIX-Sicherheits-Appliances finden Sie unter Cisco Security Appliance System Log Messages. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie unter Catalyst Switches der Serie 6500 und Cisco Router der

Serie 7600 Firewall Services Module Logging Configuration (Protokollierungskonfiguration) und System Log Messages (Systemprotokollmeldungen).

### Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die Firewall-Syslog-Meldung *106021* wird für Pakete generiert, die von Unicast RPF abgelehnt wurden. Weitere Informationen zu dieser Syslog-Meldung finden Sie unter Cisco Security Appliance System Log Message - 106021.

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 oder die Cisco Security Appliance der Serie PIX 500 finden Sie unter Configuring Logging (Konfigurieren der Protokollierung) auf der Cisco Security Appliance. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie unter Configuring Monitoring and Logging on the Cisco FWSM.

Im folgenden Beispiel **zeigt** die **Protokollierung | grep** *regex* extrahiert Syslog-Meldungen aus dem Protokollierungspuffer der Firewall. Diese Meldungen enthalten zusätzliche Informationen zu abgelehnten Paketen, die auf Versuche hinweisen könnten, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Es ist möglich, verschiedene reguläre Ausdrücke mit dem **grep-**Schlüsselwort zu verwenden, um nach bestimmten Daten in den protokollierten Nachrichten zu suchen.

Weitere Informationen zur Syntax regulärer Ausdrücke finden Sie unter Verwenden der Befehlszeilenschnittstelle.

```
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#
```

Der Befehl **show asp drop** kann außerdem die Anzahl der Pakete identifizieren, die von Unicast RPF verworfen wurden. Dies wird im folgenden Beispiel veranschaulicht:

```
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#
```

Im vorherigen Beispiel hat Unicast RPF **11 IP-Pakete** verworfen, die an Schnittstellen mit konfiguriertem Unicast RPF empfangen wurden.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie in der Cisco Security Appliance Command Reference für **show asp drop** .

## Cisco Intrusion Prevention System

## Eindämmung: Cisco IPS-Signaturereignisaktionen

Administratoren können die Appliances und Dienstmodule des Cisco Intrusion Prevention System (IPS) verwenden, um Bedrohungen zu erkennen und Versuche zu verhindern, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Diese Schwachstellen können durch die folgenden Signaturen entdeckt werden:

- 5912/0 - CUCM SIP INVITE UDP-Diensteverweigerung
- 5910/0 - CUCM Centralized TFTP File Locator Service-Pufferüberlauf

### 5912/0 - CUCM SIP INVITE UDP Denial of Service (Diensteverweigerung)

Beginnend mit dem Signatur-Update S307 für Sensoren, auf denen Cisco IPS 6.x oder 5.x ausgeführt wird, können die in diesem Dokument beschriebenen Schwachstellen mit der Signatur 6912/0 (Signature Name: CUCM Centralized TFTP File Locator Service Buffer Overflow) erkannt werden. Signatur 5912/0 ist standardmäßig aktiviert, löst ein Ereignis mit *mittlerem* Schweregrad aus, weist eine Signaturtreue (SFR) von 80 auf und ist mit der Standardereignisaktion "**Warnmeldung erzeugen**" konfiguriert. Signatur 5912/0 wird ausgelöst, wenn mehrere über den UDP-Port 5060 gesendete Pakete erkannt werden. Das Auslösen dieser Signatur kann auf eine potenzielle Ausnutzung der in diesem Dokument beschriebenen Schwachstellen hinweisen.

### 5910/0 - Pufferüberlauf beim zentralen TFTP-Dateilokalisierungs-Service für CUCM.

Beginnend mit dem Signatur-Update S307 für Sensoren, auf denen Cisco IPS 6.x oder 5.x ausgeführt wird, können die in diesem Dokument beschriebenen Schwachstellen mit der Signatur 5910/0 (Signature Name: CUCM Centralized TFTP File Locator Service Buffer Overflow) erkannt werden. Signatur 5910/0 ist standardmäßig aktiviert, löst ein Ereignis mit *mittlerem* Schweregrad aus, hat einen SFR-Wert von 75 und ist mit der Standardereignisaktion "**Warnmeldung erzeugen**" konfiguriert. Signatur 5910/0 wird ausgelöst, wenn mehrere über TCP-Port 6970 gesendete Pakete erkannt werden. Das Auslösen dieser Signatur kann auf eine potenzielle Ausnutzung der in diesem Dokument beschriebenen Schwachstellen hinweisen.

Administratoren können Cisco IPS-Sensoren so konfigurieren, dass sie eine Ereignisaktion ausführen, wenn ein Angriff erkannt wird. Die konfigurierte Ereignisaktion führt eine präventive oder abschreckende Kontrolle durch, um den Schutz vor einem Angriff zu gewährleisten, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen.

Um diese Verwundbarkeit auszunutzen, ist die Etablierung des Drei-Wege-TCP-Handshake erforderlich, der die Möglichkeit erfolgreicher Angriffe mit gefälschten IP-Adressen sowie falsch positiven Ereignissen für die Signatur 5910/0 reduziert.

Da UDP-basierte Exploits leicht gefälscht werden können, kann ein Angriff mit gefälschten Adressen dazu führen, dass eine konfigurierte Ereignisaktion versehentlich den Datenverkehr von vertrauenswürdigen Quellen blockiert. Ereignisaktionen, die die Blockierung über ACLs oder den Befehl shun durchführen, werden in der Regel auf Sensoren konfiguriert, die im Promiscuous-Modus bereitgestellt werden.

Cisco IPS-Sensoren sind am effektivsten, wenn sie im Inline-Schutzmodus in Verbindung mit einer Ereignisaktion bereitgestellt werden. Die automatische Prävention von Sicherheitsrisiken für Cisco IPS 6.x-Sensoren, die im Inline-Schutzmodus bereitgestellt werden, bietet Schutz vor Bedrohungen durch einen Angriff, der versucht, diese Schwachstellen auszunutzen. Der Schutz vor Bedrohungen wird durch eine Standardüberschreibung erreicht, die eine Ereignisaktion "**Verbindung inline verweigern**" und "**Warnung erstellen**" für ausgelöste Signaturen mit einem

*riskRatingValue* größer als 90 ausführt. Weitere Informationen zur Risikoeinstufung und zur Berechnung des Werts finden Sie unter Cisco IPS Risk Rating Explained.

Für im Inline-Schutzmodus bereitgestellte Cisco IPS 5.x-Sensoren muss eine Ereignisaktion auf Signaturbasis konfiguriert werden. Alternativ können Administratoren eine Außerkraftsetzung konfigurieren, die eine Ereignisaktion für alle Signaturen ausführen kann, die ausgelöst werden und als eine Bedrohung mit hohem Risiko berechnet werden. Die effektivste Exploit-Prevention besteht darin, die Ereignisaktion **Verbindung verweigern** und **Warnungen** auf Sensoren **erzeugen** zu verwenden, die im Inline-Schutzmodus bereitgestellt werden.

### Identifizierung: IPS-Signaturereignisse

### 5912/0 - CUCM SIP INVITE UDP Denial of Service (Diensteverweigerung)

```
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
```

### 5910/0 - Pufferüberlauf beim zentralen TFTP-Dateilokalisierungs-Service für CUCM.

```
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 Security Monitoring, Analysis and Response System]

**Identifikation: Abfragetyp und Schlüsselwort für Cisco Security Monitoring, Analysis and Response System**

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance kann Ereignisse für die CUCM-Schwachstellen bei Denial-of-Service mit einem Abfragetyp und einem Schlüsselwort abfragen. Verwenden eines Schlüsselworts NR-5912/0 für IPS-Signatur **5912/0,** das die Diensteverweigerungsschwachstelle SIP INVITE UDP erkennen kann; Schlüsselwort **NR-5910/0** für IPS-Signatur **5910/0,** das die zentrale TFTP-Datei Schwachstellen bei Service-Überläufen und ein Abfragetyp "**Alle übereinstimmenden Ereignis-Rohmeldungen"** auf der Cisco Security MARS Appliance liefern einen Bericht, der die von der IPS-Signatur 5912/0 oder 5910/0 erstellten Ereignisse auflistet.

Der folgende Screenshot zeigt die Werte, die zum Abfragen von Ereignissen verwendet werden, die von der IPS-Signatur 5912/0 (Signaturname: CUCM SIP INVITE UDP Denial of Service) oder der IPS-Signatur 5910/0 (Signaturname: CUCM Centralized TFTP File Locator Service Buffer Overflow) erstellt wurden.

Der folgende Screenshot zeigt die Abfrageergebnisse für **NR-5912/0 oder NR-5910/0,** die von der Cisco Security MARS-Appliance mithilfe eines Abfragetyps und einer Abfrage mit dem Schlüsselwort "regex" erstellt wurden.

# Zusätzliche Informationen

Dieses Dokument wird in der vorliegenden Form bereitgestellt und impliziert keine Garantie oder Gewährleistung, einschließlich der Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Die Nutzung der Informationen im Dokument oder den Materialien, die mit dem Dokument verknüpft sind, erfolgt auf Ihr eigenes Risiko. Cisco behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zu aktualisieren.

# Revisionsverlauf

| | | |
|---|---|---|
| Version 1.2 | 22. Oktober 2007 | Zugewiesene CVE-Namen einschließen |
| Version 1.1 | 17. Oktober 2007 | Informationen zum IPS-Signaturpaket S307 einfügen |
| Version 1.0 | 17. Oktober 2007 | Erste öffentliche Veröffentlichung |

# Cisco Sicherheitsverfahren

Vollständige Informationen zur Meldung von Sicherheitslücken in Cisco Produkten, zum Erhalt von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dies beinhaltet Anweisungen für Presseanfragen bezüglich der Sicherheitshinweise von Cisco. Alle Cisco Sicherheitsankündigungen finden Sie unter http://www.cisco.com/go/psirt.

## Zugehörige Informationen

- Cisco Applied Mitigation Bulletins
- Protecting Your Core: Infrastructure Protection - Zugriffskontrolllisten
- Transit-Zugriffskontrolllisten: Filterung am Netzwerk-Edge
- Grundlegendes zur Protokollierung von Zugriffskontrolllisten
- Grundlagen der Unicast Reverse Path Forwarding
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Unicast Reverse Path Forwarding Loose Mode
- Common Vulnerabilities and Exposures (CVE)
- Cisco Intrusion Prevention System 6.x
- Cisco IPS-Risikobewertung erklärt
- Cisco IPS 6.x - Signatur-Downloads
- Cisco IPS-Signaturen nach Releaseversion (nur registrierte Kunden)
- Cisco IPS-Signaturen nach Signature-ID (nur registrierte Kunden)
- Cisco Security Monitoring, Analysis and Response System

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.