Identifikation und Beseitigung von Denial-of-Service-Schwachstellen in Cisco Unified Communications Manager und Cisco Intercompany Media Engine

Identifikation und Beseitigung von Denial-of-Service-Schwachstellen in Cisco Unified Communications Manager und Cisco Intercompany Media Engine

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

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

Version 1.1

Zuletzt aktualisiert am 2011. November 2012 um 23:20 Uhr UTC (GMT)

Zur öffentlichen Veröffentlichung 2011 24. August 00:00 UTC (GMT)

Inhalt

Antwort von Cisco

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

Merkmale der Schwachstelle

Cisco Unified Communications Manager und die Intercompany Media Engine weisen mehrere Schwachstellen auf. Die folgenden Unterabschnitte fassen diese Schwachstellen zusammen:**DoS-Schwachstelle in Cisco Unified Communications Manager mit aktiviertem Packet Capture Service:** Diese Schwachstelle kann per Fernzugriff ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Wenn diese Schwachstelle erfolgreich ausgenutzt

wird, kann das betroffene Gerät abstürzen. Wiederholte Versuche, diese Schwachstelle auszunutzen, könnten zu einer anhaltenden Denial of Service (DoS)-Situation führen, wenn der Speicher des Unified Communications Manager aufgebraucht wird. Der Angriffsvektor zur Ausnutzung besteht in TCP-Paketen, die einen Drei-Wege-TCP-Handshake an den Unified Communications Manager abschließen und die Verbindungen offen lassen.Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-2560 zugewiesen.**DoS-Schwachstelle in Cisco Unified Communications Manager mit bestimmten MTP-Konfigurationen:** Diese Schwachstelle kann per Fernzugriff ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann das betroffene Gerät abstürzen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen.Die Angriffsvektoren zur Ausnutzung werden durch Pakete generiert, die die folgenden Protokolle und Ports verwenden:

- Session Initiation Protocol (SIP) mit TCP-Port 5060
- SIP über Transport Layer Security (TLS) mit TCP-Port 5061
- SIP mit UDP-Port 5060
- SIP mit UDP-Port 5061

Ein Angreifer könnte diese Schwachstellen mithilfe gefälschter Pakete ausnutzen.Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-2561 zugewiesen.**DoS-Schwachstelle im Cisco Unified Communications Manager bei der Verarbeitung bestimmter SIP-INVITE-Nachrichten:** Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann das betroffene Gerät abstürzen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen.Die Angriffsvektoren zur Ausnutzung werden durch Pakete generiert, die die folgenden Protokolle und Ports verwenden:

- SIP über TCP-Port 5060
- SIP-TLS über Transport Layer Security (TLS) mit TCP-Port 5061
- SIP mit UDP-Port 5060
- SIP-TLS mit UDP-Port 5061

Ein Angreifer könnte diese Schwachstellen mithilfe gefälschter Pakete ausnutzen.Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-2562 zugewiesen.**Zwei DoS-Schwachstellen in Cisco Unified Communications Manager und Cisco Intercompany Media Engine (IME) mit Service Advertisement Framework (SAF)**: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann das betroffene Gerät abstürzen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen.Die Angriffsvektoren für die Ausnutzung sind wie folgt aufgebaut:

- SAF-Pakete über TCP-Ports 5050 (für Cisco Unified Communications Manager)
- SAF-Pakete über TCP-Port 5620 (für IME)

Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2011-2563 und CVE-2011-2564 zugewiesen.Informationen zu anfälliger, nicht betroffener und fester Software finden Sie in den PSIRT-Sicherheitsempfehlungen unter den folgenden Links: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-cucm und https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-ime.

Überblick über die Risikominderungstechnik

Cisco Geräte bieten eine Reihe von Gegenmaßnahmen für diese Sicherheitslücken. Den Administratoren wird empfohlen, diese Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs im Netzwerk zu betrachten. Dieser Abschnitt des Dokuments bietet einen Überblick über diese Techniken.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, diese Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.Die ordnungsgemäße Bereitstellung und Konfiguration von Unicast RPF bietet einen effektiven Schutz vor Angriffen, bei denen Pakete mit gefälschten Quell-IP-Adressen verwendet werden. Unicast-RPF sollte so nahe wie möglich an allen Datenverkehrsquellen bereitgestellt werden.Die ordnungsgemäße Bereitstellung und Konfiguration von IPSG bietet einen effektiven Schutz vor Spoofing-Angriffen auf der Zugriffsebene.Da die Möglichkeit besteht, dass ein vertrauenswürdiger Netzwerk-Client von einem Wurm betroffen sein könnte, der keine Pakete mit gefälschten Quelladressen verwendet, bieten Unicast RPF und IPSG keinen vollständigen Schutz vor diesen Schwachstellen.Die Cisco Adaptive Security Appliance der Serie ASA 5500 und das Firewall Services Module (FWSM) für Cisco Catalyst 6500 sorgen zudem für einen effektiven Schutz vor Bedrohungen.

- Transit-Zugriffskontrolllisten (tACLs)
- Unicast Reverse Path Forwarding (Unicast-RPF)
- TCP-Normalisierung

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.Die Cisco ACE Application Control Engine Appliance und das Cisco ACE-Modul bieten zudem über die TCP-Normalisierung einen effektiven Schutz vor Sicherheitslücken.Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstellen auszunutzen.Die effektive Nutzung von Cisco Intrusion Prevention System (IPS)-Ereignisaktionen bietet Transparenz und Schutz vor Angriffen, die diese Schwachstellen ausnutzen.Cisco IOS NetFlow-Datensätze bieten Transparenz für netzwerkbasierte Exploit-Versuche.Die Cisco IOS Software, die Cisco ASA, die FWSM-Firewalls sowie die

Cisco ACE Application Control Engine Appliance und das Cisco ACE-Modul bieten Transparenz durch Syslog-Meldungen und Zählerwerte, die in der Ausgabe der **show-**Befehle angezeigt werden.Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance bietet ebenfalls Transparenz für Vorfälle, Abfragen und Ereignisberichte.

Risikomanagement

Unternehmen wird empfohlen, ihre standardmäßigen Risikobewertungs- und Minderungsprozesse zu befolgen, um die potenziellen Auswirkungen von [dieser Schwachstelle|diesen 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 Ankündigungen zu Sicherheitslücken sowie Risikoanalyse und -prototyping unterstützen Unternehmen bei der Entwicklung wiederholbarer Sicherheitsevaluierungs- und Reaktionsprozesse.

Gerätespezifische Eindämmung und Identifizierung

Vorsicht: Die Effektivität jeglicher Eindämmungstechnik 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 und FWSM-Firewalls
- Cisco ACE
- 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 am Eingangspunkt in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Verbindungspunkte für Partner und Lieferanten 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. Eine tACL-Problemumgehung kann keinen vollständigen Schutz vor diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.Die tACL-Richtlinie verweigert nicht autorisierte SIP-, SAF- und SIP-TLS-Pakete an den TCP- und UDP-Ports 5060 und 5061, die an betroffene Geräte gesendet werden. Im folgenden Beispiel sind 192.168.60.0/24 und 2001:DB8:1:60::/64 der IPv4- bzw. IPv6-Adressraum, der von den betroffenen Geräten verwendet wird, und der Host mit 192.168.100.1 (2001:DB8:1:101) 0::1 für IPv6) 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 in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable protocols and ports ! access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 access-list 150 deny deny
```

```
tcp any 192.168.60.0 0.0.0.255 eq 5620 ! !-- Permit or deny all other Layer 3
and Layer 4 traffic in accordance !-- with existing security policies and
configurations ! !-- Explicit deny for all other IP traffic ! access-list 150
deny ip any any ! !-- Create the corresponding IPv6 tACL ! ipv6 access-list
IPv6-Infrastructure-ACL-Policy ! !-- Include explicit permit statements for
trusted sources !-- that require access on the vulnerable protocols and ports
! permit tcp host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit tcp
host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5050 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks to global and !-- link local addresses ! deny tcp
any 2001:DB8:1:60::/64 eq 5060 deny tcp any 2001:DB8:1:60::/64 eq 5061 deny
udp any 2001:DB8:1:60::/64 eq 5060 deny udp any 2001:DB8:1:60::/64 eq 5061
deny tcp any 2001:DB8:1:60::/64 eq 5050 deny tcp any 2001:DB8:1:60::/64 eq
5620 ! !-- Permit other required traffic to the infrastructure address !--
range and allow IPv6 Neighbor Discovery packets, which !-- include Neighbor
Solicitation packets and Neighbor !-- Advertisement packets ! permit icmp any
any nd-ns permit icmp any any nd-na ! !-- Explicit deny for all other IP
traffic to the global !-- infrastructure address range ! deny ipv6 any
2001:DB8:1:60::/64 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic
!-- in accordance with existing security policies and configurations ! ! !--
Apply tACLs to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group 150 in ipv6 traffic-filter IPv6-
Infrastructure-ACL-Policy in
```

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** *unreachableIntervall-in-ms* vom Standard *geändert werden*.

Eindämmung: Spoofing-SchutzUnicast Reverse Path Forwarding Die in diesem Dokument beschriebenen Schwachstellen können durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast Reverse Path Forwarding (Unicast RPF) als Schutzmechanismus gegen Spoofing bereitstellen und konfigurieren.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 vollständigen 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. Den Administratoren wird empfohlen, während der Bereitstellung dieser Funktion sicherzustellen, dass 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. Bei ordnungsgemäßer Bereitstellung und Konfiguration bietet IPSG in Verbindung mit dem Unicast RPF im strikten Modus den effektivsten Spoofing-Schutz für die in diesem Dokument beschriebenen Schwachstellen.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- und SIP-TLS-Pakete an den TCP- und UDP-Ports 5060 und 5061, die gefiltert wurden. Den Administratoren wird empfohlen, gefilterte Pakete zu 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 tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620
    70 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (5 matches)
    80 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (2 matches)
    90 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 (7 matches)
    100 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 (4 matches)
    110 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 (6 matches)
    120 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5620 (1 matches)
    130 permit icmp any any nd-ns
    140 permit icmp any any nd-ns
    150 deny ip any any
router#
```

Im vorherigen Beispiel hat die Zugriffsliste 150 die folgenden Pakete verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden:

- **5 SIP**-Pakete am **TCP-Port 5060** für ACE-Leitung 70
- **2 SIP-TLS**-Pakete am **TCP-Port 5061** für ACE-Leitung 80
- **7 SIP**-Pakete am **UDP-Port 5060** für ACE-Leitung 90
- **4 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 100
- **6 SAF**-Pakete am **TCP-Port 5050** für ACE-Leitung 110
- **1 SAF**-Paket am **TCP-Port 5620** für ACE-Leitung 120

Die entsprechende Ausgabe für IPv6 tACLs ist sehr ähnlich und wird hier aus Kurzgründen weggelassen. Weitere Informationen zur Untersuchung von Vorfällen mithilfe von ACE-Zählern und Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.Administratoren können den Embedded Event Manager verwenden, um eine Instrumentierung bereitzustellen, wenn bestimmte Bedingungen erfüllt sind, z. B. ACE-Zählerzugriffe. Das Whitepaper Embedded Event Manager in a Security Context von Applied Intelligence enthält weitere Informationen zur Verwendung dieser Funktion.**Identifizierung: Protokollierung der Zugriffsliste**Die Option **log** and **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 für die Weiterleitung von Paketen, die mit protokollfähigen ACEs übereinstimmen.Bei Cisco IOS-Software kann der Befehl **ip access-list logging interval** *interval-in-ms* 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.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.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 implementiert und konfiguriert ist, können Administratoren den *Steckplatz/Port des* Schnittstellentyps "show cef", *die* **Befehle "show ip interface", "show cef drop",** die **Funktion "show ip cef switching statistics"** und "**show ip traffic" verwenden,um die Anzahl der von Unicast RPF blockierten Pakete zu identifizieren.Hinweis:** Ab Version 12.4(20)T der Cisco IOS-Software wurde der Befehl **show ip cef switching** durch die **Funktion show ip cef switching statistics** ersetzt.**Hinweis: Die Befehle show | begin** *regex* und **show** *command* **| include** *regex***-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 den Abschnitten show command in der Cisco IOS Configuration Fundamentals Command Reference.

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

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

```
router#
```

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

```
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#
```

Im vorhergehenden Abschnitt **show cef drop**, **show ip cef switching statistics feature** and **show ip traffic** example, Unicast RPF hat **18 global empfangene IP-Pakete** an allen Schnittstellen mit konfigurierter Unicast RPF verworfen, weil die Quelladresse der IP-Pakete in der Forwarding Information Base von Cisco Express Forwarding nicht verifiziert werden konnte.**Cisco IOS-NetFlowIdentifizierung: Identifikation des Datenverkehrsflusses mithilfe von NetFlow-Datensätzen**Administratoren können Cisco IOS NetFlow auf Cisco IOS-Routern und -Switches konfigurieren, um Datenverkehrsflüsse zu identifizieren, die diese Schwachstellen ausnutzen können. Den Administratoren wird empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen, oder ob es sich um legitime Datenflüsse handelt.

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
```

```
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für SIP-, SAF- und SIP-TLS-Pakete auf den TCP-Ports 5060 (Hexadezimalwert 13C4), 5061 (Hexadezimalwert 13C5), 5050 (Hexadezimalwert 13BA) und 5620 (Hexadezimalwert 1 5F4) und UDP-Ports 5060 (Hexadezimalwert 13C4) und **5061 (Hexadezimalwert 13C5)**.Dieser Datenverkehr wird von Adressen im Adressblock 192.168.60.0/24 generiert und an diese gesendet, der von den betroffenen Geräten verwendet wird. Die Pakete in diesen Flows können gefälscht sein und einen Versuch anzeigen, diese Schwachstellen auszunutzen. Den Administratoren wird empfohlen, diese Datenflüsse mit der Basisauslastung für den SIP- und SIP-TLS-Datenverkehr auf den UDP-Ports 5060 und 5061 zu vergleichen und sie zu untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.Um nur die Datenverkehrsflüsse für SIP-, SAF- und SIP-TLS-Pakete auf den TCP-Ports 5060 (Hexadezimalwert 13C4), 5061 (Hexadezimalwert 13C5), 5050 (Hexadezimalwert 13BA) und 5620 (Hexadezimalwert 15F4) anzuzeigen, muss der folgende Befehl ausgeführt werden: IP-Cache-Fluss anzeigen **| include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_** zeigt die zugehörigen UDP NetFlow-Datensätze wie folgt an:**TCP-Flows**

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

Um nur die Datenverkehrsflüsse für SIP- und SIP-TLS-Pakete auf den UDP-Ports 5060 (Hexadezimalwert 13C4) und 5061 (Hexadezimalwert 13C5) anzuzeigen, wird der **IP-Cache-Fluss angezeigt. | include SrcIf|_11_.*(13C4|13C5)_** zeigt die zugehörigen UDP NetFlow-Datensätze wie folgt an:**UDP-Datenflüsse**

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

Identifizierung: Identifikation des Datenverkehrsflusses mithilfe von IPv6 NetFlow-Datensätzen Administratoren können Cisco IOS IPv6 NetFlow auf Cisco IOS-Routern und -Switches konfigurieren, um Datenverkehrsflüsse zu identifizieren, bei denen möglicherweise versucht wird, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Den Administratoren wird

empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen, oder ob es sich um legitime Datenflüsse handelt.Diese Ausgabe stammt von einem Cisco IOS-Gerät, auf dem die Cisco IOS-Software 12.4 Mainline Train ausgeführt wird. Die Befehlssyntax variiert je nach Cisco IOS-Software.

```
router#show ipv6 flow cache
IP packet size distribution (50078919 total packets):
   1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .990 .001 .008 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

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

Um die Anzeige der vollständigen 128-Bit-IPv6-Adresse zu ermöglichen, verwenden Sie den Befehl **terminal width 132** exec mode.Im vorherigen Beispiel gibt es mehrere Datenflüsse für SIP-, SAF- und SIP-TLS-Pakete auf den TCP-Ports 5060 (Hexadezimalwert 13C4), 5061 (Hexadezimalwert 13C5), 5050 (Hexadezimalwert 13BA) und 5620 (Hexadezimalwert 1 5F4) und UDP-Ports 5060 (Hexadezimalwert 13C4) und **5061 (Hexadezimalwert 13C5)**.Dieser Datenverkehr wird an Adressen im Adressblock 2001:DB8:1:60::/64 gesendet, der von den betroffenen Geräten verwendet wird. Die Pakete in diesen Flows können gefälscht sein und einen Versuch anzeigen, diese Schwachstellen auszunutzen. Den Administratoren wird empfohlen, diese Datenflüsse mit der Basisauslastung für den SIP- und SIP-TLS-Datenverkehr auf den UDP-Ports 5060 und 5061 zu vergleichen und sie zu untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.Wie im folgenden Beispiel gezeigt, um nur die SIP-, SAF- und SIP-TLS-Pakete auf den TCP-Ports 5060 (Hexadezimalwert 13C4), 5061 (Hexadezimalwert 13C5), 5050 (Hexadezimalwert 13BA) und 5620 (Hexadezimalwert 15F4) anzuzeigen, Verwenden Sie den **show ipv6 flow cache. | include SrcAddress|_06_.*(13C4|13C5|13BA|15F4)_** command to display the related NetFlow records:

TCP-Flows

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

Um nur SIP- und SIP-TLS-Datenverkehrsflüsse für den IPv6-UDP-Port 5060 (**Hexadezimalwert 0x13C4)** und 5061 (**Hexadezimalwert 0x13C5)** anzuzeigen, verwenden Sie **show ipv6 flow cache | include SrcAddress|_11_.*(13C4|13C5)_** command to display the related NetFlow records:**UDP-Datenflüsse**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
```

```
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
routter#
```

Cisco ASA und FWSM-Firewalls **Eindämmung: Transit-Zugriffskontrolllisten** Um das Netzwerk vor Datenverkehr zu schützen, der am Eingangspunkt in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Verbindungspunkte für Partner 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. Eine tACL-Problemumgehung kann keinen vollständigen Schutz vor diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.Die tACL-Richtlinie verweigert nicht autorisierte SIP-, SAF- und SIP-TLS-Pakete an den TCP- und UDP-Ports 5060 und 5061, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 und 2001:DB8:1:60::/64 der IPv4- bzw. IPv6-Adressraum, der von den betroffenen Geräten verwendet wird, sowie der Host unter 192.168.100.1 (2001:DB8:1:101) 0::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 in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require
access on the vulnerable protocols and ports ! access-list tACL-Policy
extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 access-list tACL-Policy extended permit udp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy
extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5050 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended deny tcp
any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny
udp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended
deny udp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-
Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5620 ! !-- Permit
or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP
traffic ! access-list tACL-Policy extended deny ip any any ! !-- Include
explicit permit statements for trusted sources !-- that require access on the
vulnerable protocols and ports ! ipv6 access-list IPv6-tACL-Policy permit tcp
host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-
Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1
2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit udp host
2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-
Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5050 ipv6
access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1
2001:db8:1:60::/64 eq 5620 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5060 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5060 ipv6
access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5050 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5620 ! !--
Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Explicit deny for all
other IP traffic ! ipv6 access-list IPv6-Transit-ACL-Policy deny ip any any
```

```
! !-- Apply tACLs to interfaces in the ingress direction ! access-group tACL-Policy in interface outside access-group IPv6-Transit-ACL-Policy in interface outside
```

Eindämmung: Spoofing-Schutz mit Unicast Reverse Path Forwarding Die in diesem Dokument beschriebenen Schwachstellen können durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast RPF als Spoofing-Schutzmechanismus bereitstellen und konfigurieren.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 vollständigen 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.**Abschwächung: TCP-Normalisierung**Die TCP-Normalisierungsfunktion identifiziert ungewöhnliche Pakete, auf die die Sicherheits-Appliance reagieren kann, wenn sie erkannt werden. Beispielsweise kann die Sicherheits-Appliance die Pakete zulassen, verwerfen oder löschen. Der TCP-Normalisierer umfasst nicht konfigurierbare und konfigurierbare Aktionen. Normalerweise werden Pakete, die als schädlich eingestuft werden, durch nicht konfigurierbare Aktionen zum Verwerfen oder Löschen von Verbindungen betroffen. Die TCP-Normalisierung ist ab Softwareversion 7.0(1) für die Cisco Adaptive Security Appliance der Serie ASA 5500 und ab Softwareversion 3.1(1) für das Firewall Services Module verfügbar.Die TCP-Normalisierung ist standardmäßig aktiviert und löscht Pakete, die diese Schwachstellen ausnutzen können. Der Schutz vor Paketen, die diese Schwachstellen ausnutzen, ist eine nicht konfigurierbare TCP-Normalisierungsaktion. Konfigurationsänderungen sind nicht erforderlich, um diese Funktion zu aktivieren.Die TCP-Normalisierungsfunktion kann verwendet werden, um die gleichzeitige Verbindungsbeschränkung und die Leerlaufzeitüberschreitung für TCP-Verbindungen mit dem Cisco Unified Communications Manager zu begrenzen und so die DoS-Bedingung zu verhindern. Die Grenzwerte sollten entsprechend der maximalen normalen Anzahl von Verbindungen konfiguriert werden, die in Richtung Cisco Unified Communications Manager beobachtet werden. Der Leser sollte beachten, dass die Konfiguration des TCP-Normalisierungsprogramms, um eine ungewöhnliche Anzahl von Verbindungen zum Cisco Unified Communications Manager zu verhindern, einen dauerhaften Angreifer nicht daran hindert, die zulässige Anzahl von Verbindungen zu erschöpfen. Sie verhindert jedoch, dass dem Cisco Unified Communications Manager aufgrund zahlreicher inaktiver Verbindungen der Arbeitsspeicher ausgeht.**Hinweis:** Die in den einzelnen Umgebungen festgelegten Grenzwerte müssen eingehalten werden, da legitime Verbindungen verweigert werden können, wenn die legitimen Grenzwerte für die jeweilige Umgebung nicht eingehalten werden.Im folgenden Beispiel ist 192.168.60.200/24 die IP-Adresse des betroffenen Geräts. Die Konfiguration schränkt die Anzahl gleichzeitiger TCP-Verbindungen zum Gerät auf 1000 ein und legt den Timeout für Verbindungsausfälle auf 30 Minuten fest. Die in den einzelnen Umgebungen festgelegten Grenzwerte sollten beachtet werden, da legitime Verbindungen verweigert werden können, wenn die normalen Höchstwerte für die jeweilige Umgebung nicht eingehalten werden.

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

Weitere Informationen zur TCP-Normalisierung finden Sie im Abschnitt Configuring TCP Normalization im Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2.**Identifizierung: Transit-Zugriffskontrolllisten**Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der SIP- und SIP-TLS-Pakete auf den TCP- und UDP-Ports 5060 und 5061 identifizieren, die gefiltert wurden. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show access-list tACL-Policy**:

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

```
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=44)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=61)
access-list tACL-Policy line 7 extended deny tcp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=5)
access-list tACL-Policy line 8 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
access-list tACL-Policy line 9 extended deny udp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=7)
access-list tACL-Policy line 10 extended deny udp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=4)
access-list tACL-Policy line 11 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5050 (hitcnt=6)
access-list tACL-Policy line 12 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5620 (hitcnt=1)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=8)
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste *tACL-Policy* die folgenden Pakete verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden:

- **5 SIP**-Pakete am **TCP-Port 5060** für ACE-Leitung 7
- **2 SIP-TLS**-Pakete am **TCP-Port 5061** für ACE-Leitung 8
- **7 SIP**-Pakete am **UDP-Port 5060** für ACE-Leitung 9
- **4 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 10
- **6 SAF**-Pakete am **TCP-Port 5050** für ACE-Leitung 11
- **1 SAF**-Pakete am **TCP-Port 5620** für ACE-Leitung 12

Die entsprechenden Ausgaben für IPv6 tACLs sind sehr ähnlich und werden hier aus Gründen der Kürze weggelassen.

Identifizierung: Firewall Access List, 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 in Cisco ASA 5500 Series System Log Message, 8.2 - 106023.Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 finden Sie unter Überwachung - Konfigurieren der Protokollierung. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie im Monitoring the Firewall Services Module.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 potenzielle 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 Erstellen eines regulären Ausdrucks.

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

Im vorherigen Beispiel zeigen die für die tACL-*tACL-Richtlinie* protokollierten Meldungen potenziell gefälschte **SIP- und SIP-TLS-**Pakete für die **TCP- und UDP-Ports 5060 und 5061 an,** die an den betroffenen Geräten zugewiesenen Adressblock gesendet wurden.Weitere Informationen zu Syslog-Meldungen für ASA Security Appliances finden Sie in Cisco ASA 5500 Series System Log

Messages, 8.2. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie in den Protokollnachrichten des Catalyst Switches der Serie 6500 und des Cisco Routers der Serie 7600, Protokollierungssystem für Firewall-Services-Module.Weitere Informationen zur Untersuchung von Vorfällen mithilfe von Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.**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 in Cisco ASA 5500 Series System Log Message, 8.2 - 106021.Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 finden Sie unter Überwachung - Konfigurieren der Protokollierung. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie im Monitoring the Firewall Services Module.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 potenzielle 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 Erstellen eines regulären Ausdrucks.

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

Der Befehl **show asp drop** kann außerdem die Anzahl der Pakete identifizieren, die von der Unicast RPF-Funktion verworfen wurden, wie im folgenden Beispiel gezeigt:

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

Im vorherigen Beispiel hat Unicast RPF **11 IP-Pakete** verworfen, die an Schnittstellen mit konfiguriertem Unicast RPF empfangen wurden. Fehlende Ausgabe zeigt an, dass die Unicast-RPF-Funktion der Firewall keine Pakete verworfen hat.Weitere Informationen zum Debuggen von Paketen oder Verbindungen, die über einen beschleunigten Sicherheitspfad verworfen wurden, finden Sie unter Cisco Security Appliance Command Reference (Cisco Security Appliance-Befehlsreferenz) für show asp drop.
Identifizierung: TCP-NormalisierungFür die Cisco Adaptive Security Appliance der Serie ASA 5500 kann der Befehl **show service-policy** die Anzahl der Pakete identifizieren, die durch die TCP-Normalisierungsfunktion verloren gegangen sind, wie im folgenden Beispiel gezeigt:

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

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

Im vorherigen Beispiel wurden bei der TCP-Normalisierung **5 neue Verbindungen** abgebrochen, die den Verbindungsgrenzwert überschritten.**Cisco ACE****Abschwächung: TCP-Normalisierung**Die TCP-Normalisierung ist eine Layer-4-Funktion, die aus einer Reihe von Prüfungen besteht, die der Cisco ACE in verschiedenen Phasen eines Datenflusses durchführt, beginnend mit der anfänglichen Verbindungseinrichtung bis hin zum Schließen einer Verbindung. Viele der Segmentprüfungen können durch Konfigurieren einer oder mehrerer erweiterter TCP-Verbindungseinstellungen gesteuert oder geändert werden. Der ACE entscheidet anhand dieser TCP-Verbindungseinstellungen, welche Prüfungen durchgeführt werden und ob ein TCP-Segment aufgrund der Ergebnisse der Prüfungen verworfen werden soll. Der ACE verwirft Segmente, die anormal oder fehlerhaft zu sein scheinen.Die TCP-Normalisierung ist standardmäßig aktiviert und löscht Pakete, die diese Schwachstellen ausnutzen können. Der Schutz vor Paketen, die diese Schwachstellen ausnutzen, ist eine nicht konfigurierbare TCP-Normalisierungsaktion. Zum Aktivieren dieser Funktion sind keine Konfigurationsänderungen erforderlich.Die TCP-Normalisierungsfunktion kann verwendet werden, um die Anzahl gleichzeitiger Verbindungen, die Verbindungsrate und die Leerlaufzeitüberschreitung für TCP-Verbindungen mit dem Cisco Unified Communications Manager zu begrenzen und so den DoS-Zustand zu verhindern. Die Grenzwerte müssen

entsprechend der maximalen Anzahl normaler Verbindungen konfiguriert werden, die für den Cisco Unified Communications Manager beobachtet werden. Der Leser sollte beachten, dass die Konfiguration des TCP-Normalisierungsprogramms, um eine ungewöhnliche Anzahl von Verbindungen zum Cisco Unified Communications Manager zu verhindern, einen dauerhaften Angreifer nicht daran hindert, die zulässige Anzahl von Verbindungen zu erschöpfen. Sie verhindert jedoch, dass dem Cisco Unified Communications Manager aufgrund zahlreicher inaktiver Verbindungen der Arbeitsspeicher ausgeht.**Hinweis:** Die in den einzelnen Umgebungen festgelegten Grenzwerte müssen eingehalten werden, da legitime Verbindungen verweigert werden können, wenn die legitimen Grenzwerte für die jeweilige Umgebung nicht eingehalten werden.Im folgenden Beispiel ist 192.168.60.200/24 die IP-Adresse des betroffenen Geräts. Die Konfiguration begrenzt die Anzahl gleichzeitiger TCP-Verbindungen zum Gerät auf 1.000, die Verbindungsrate auf 100000 Verbindungen pro Sekunde und legt den Timeout bei Verbindungsausfällen auf 30 Minuten fest.

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

Weitere Informationen zur TCP-Normalisierung finden Sie im Abschnitt Configuring TCP/IP Normalization and IP Reassembly Parameters im Cisco ACE 4700 Series Appliance Security Configuration Guide.**Identifizierung: TCP-Normalisierung**Die Cisco ACE Application Control Engine Appliance und das Modul bieten keine Ausgabe von show-Befehlen für Pakete, die beim Versuch, diese Schwachstellen auszunutzen, verworfen wurden.**Cisco Intrusion Prevention System****Eindämmung: Cisco IPS-Signaturereignisaktionen**Administratoren können Cisco Intrusion Prevention System (IPS)-Appliances und -Servicemodule verwenden, um eine Erkennung von Sicherheitsrisiken zu ermöglichen und Versuche zu verhindern, eine der in diesem Dokument beschriebenen Schwachstellen auszunutzen. Beginnend mit dem Signatur-Update S590 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, kann die Schwachstelle mit der Signatur 38386/0 erkannt werden (Signature Name: Cisco Intercompany Media Engine Denial of Service). Signatur 38386/0 ist standardmäßig aktiviert, löst ein Ereignis mit *mittlerem* Schweregrad aus, hat eine Signaturtreue-Bewertung (SFR) von 15 und wird mit einer Standardereignisaktion **von Produce Alert** konfiguriert.Signatur 38386/0 wird ausgelöst, wenn bestimmte schädliche Pakete erkannt werden, die über den TCP-Port 5620 gesendet werden. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken 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.Exploits, die gefälschte IP-Adressen verwenden, können dazu führen, dass eine konfigurierte Ereignisaktion versehentlich den Datenverkehr von vertrauenswürdigen Quellen blockiert.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 und höhere Sensoren, die im Inline-Schutzmodus bereitgestellt werden, bietet Schutz vor Bedrohungen bei einem Angriff, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Der Schutz vor Bedrohungen wird durch eine Standardüberschreibung erreicht, die eine Ereignisaktion für ausgelöste Signaturen mit einem *riskRatingValue* größer als 90 ausführt.Weitere Informationen zur Berechnung von Risikoeinstufung und Bedrohungseinstufung finden Sie unter Risikoeinstufung und Bedrohungseinstufung: Vereinfachtes IPS-Richtlinienmanagement.**Cisco Security Monitoring, Analysis and Response System****Identifikation: Cisco Security Monitoring, Analysis, and Response System Incidents**Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance kann Incidents zu Ereignissen erstellen, die mit den in diesem Dokument beschriebenen Schwachstellen zusammenhängen. Hierzu wird die IPS-Signatur 38386/0 (Signature Name: Cisco Intercompany Media Engine Denial of Service) verwendet. Nach dem Download des dynamischen Signatur-Updates für S590 mithilfe des Schlüsselworts **NR-38386/0** für die IPS-Signatur 38386/0 und des Abfragetyps **< Alle übereinstimmenden Ereignisse | Alle Matching Event Raw Messages>** auf der Cisco Security MARS Appliance liefert einen Bericht, in dem die durch die IPS-Signatur erstellten Incidents aufgeführt sind.Ab der Version 4.3.1 und 5.3.1 der Cisco Security MARS-Appliances wird die Funktion zur Aktualisierung dynamischer Signaturen von Cisco IPS unterstützt. Diese Funktion lädt neue Signaturen von Cisco.com oder von einem lokalen Webserver herunter, verarbeitet und kategorisiert empfangene Ereignisse, die mit diesen Signaturen übereinstimmen, ordnungsgemäß und fügt sie in Prüfungsregeln und Berichte ein. Diese Updates ermöglichen die Ereignisnormalisierung und die Zuordnung von Ereignisgruppen. Außerdem können neue Signaturen von IPS-Geräten mithilfe der MARS-Appliance analysiert werden.**Achtung:** Wenn keine dynamischen Signaturaktualisierungen konfiguriert sind, werden Ereignisse, die diesen neuen Signaturen entsprechen, in Abfragen und Berichten als *unbekannter Ereignistyp* angezeigt. Da MARS diese Ereignisse nicht in die Überprüfungsregeln einbezieht, kann es vorkommen, dass keine Vorfälle für potenzielle Bedrohungen oder Angriffe innerhalb des Netzwerks erstellt werden.Diese Funktion ist standardmäßig aktiviert, muss jedoch konfiguriert werden.

Wenn sie nicht konfiguriert ist, wird die folgende Cisco Security MARS-Regel ausgelöst:
`System Rule: CS-MARS IPS Signature Update Failure`
Wenn diese Funktion aktiviert und konfiguriert ist, können Administratoren die aktuelle von MARS heruntergeladene Signaturversion ermitteln, indem sie **Hilfe > Info** auswählen und den Wert für die *IPS-Signaturversion* überprüfen.Zusätzliche Informationen zu dynamischen Signatur-Updates und Anweisungen zum Konfigurieren dynamischer Signatur-Updates sind für die Versionen Cisco Security MARS 4.3.1 und 5.3.1 verfügbar.

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 1.1	2. November 2011	Korrigierte Dokument-URL
Version 1.0	24. August 2011	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
- Cisco Security
- Cisco Security IntelliShield Alert Manager Service
- Cisco Leitfaden zum Absichern von Cisco IOS-Geräten
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- NetFlow-Leistungsanalyse
- Cisco Network Foundation Protection - Whitepaper
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Cisco ACE Application Control Engine Module - Dokumentation
- Verbesserungen der Unicast Reverse Path Forwarding für den Internet Service Provider
- Cisco Intrusion Prevention System
- Cisco IPS-Signatur-Downloads
- Seite für die Suche nach Cisco IPS-Signaturen
- Cisco Security Monitoring, Analysis and Response System

- Common Vulnerabilities and Exposures (CVE)

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.