Identifizieren und Beseitigen der Ausnutzung mehrerer DoS-Schwachstellen in Cisco Unified Communications-Produkten

Identifizieren und Beseitigen der Ausnutzung mehrerer DoS-Schwachstellen in Cisco Unified Communications-Produkten

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

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

Version 1.0

Zur öffentlichen Veröffentlichung 2010 25. August 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses "Applied Mitigation Bulletin" ist ein Begleitdokument zu den PSIRT-Sicherheitsratschlägen Schwachstellen bei Denial-of-Service von Cisco Unified Communications Manager und Schwachstellen bei Denial-of-Service von Cisco Unified Presence Denial of Service und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten implementieren können.

Merkmale der Schwachstelle

Der SIP-Prozess der Produkte Cisco Unified Communications Manager und Cisco Unified Presence weist mehrere Schwachstellen auf. Die folgenden Unterabschnitte fassen diese Schwachstellen zusammen:

Sicherheitslücken in Cisco Unified Communications Manager Denial of Service (DoS): Diese Sicherheitslücken können ohne Authentifizierung und ohne Benutzereingriff aus der Ferne

ausgenutzt werden. Wenn diese Schwachstellen erfolgreich ausgenutzt werden, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstellen auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen.

Die Angriffsvektoren zur Ausnutzung werden durch SIP-Pakete generiert, die die folgenden Protokolle und Ports verwenden:

- SIP über TCP-Port 5060
- SIP über TCP-Port 5061
- SIP mit UDP-Port 5060
- SIP mit UDP-Port 5061

Ein Angreifer könnte diese Schwachstellen mithilfe gefälschter Pakete ausnutzen.

Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2010-2837 und CVE-2010-2838 zugewiesen.

Schwachstellen bei Cisco Unified Presence Denial of Service (DoS): Diese Schwachstellen können ohne Authentifizierung und ohne Benutzereingriff aus der Ferne ausgenutzt werden. Wenn diese Schwachstellen erfolgreich ausgenutzt werden, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstellen auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen.

Die Angriffsvektoren zur Ausnutzung werden durch SIP-Pakete generiert, die die folgenden Protokolle und Ports verwenden:

- SIP über TCP-Port 5060
- SIP über TCP-Port 5061
- SIP mit UDP-Port 5060
- SIP mit UDP-Port 5061

Ein Angreifer könnte diese Schwachstellen mithilfe gefälschter Pakete ausnutzen.

Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2010-2839 und CVE-2010-2840 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-20100825-cucm und https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100825-cup.

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 eine effektive Vermeidung von 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.

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.

- tACL
- Unicast RPF

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.

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 Firewalls Cisco IOS Software, Cisco ASA und FWSM 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

Den Unternehmen wird empfohlen, die potenziellen Auswirkungen dieser Schwachstellen anhand ihrer Standardprozesse zur Risikobewertung und -minderung 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 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-Pakete an den TCP-Ports 5060 und 5061 sowie den UDP-Ports 5060 und 5061, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen Geräten verwendet wird. 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 in Transit Access Control Lists: Filtering at Your Edge.

```
!-- Include explicit permit statements for trusted sources !-- that require access on
the vulnerable ports ! access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 ! !-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks ! access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
5061 access-list 150 deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny
udp any 192.168.60.0 0.0.0.255 eq 5061 ! !-- Permit or deny all other Layer 3 and
Layer 4 traffic in accordance !-- with existing security policies and configurations
! !-- Explicit deny for all other IP traffic ! access-list 150 deny ip any any ! !--
Apply tACL to interfaces in the ingress direction ! interface GigabitEthernet0/0 ip
access-group 150 in
```

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.

Eindämmung: Spoofing-Schutz

Unicast 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-Zugriffskontrollisten

Nachdem der Administrator die tACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der SIP-Pakete an den TCP-Ports 5060 und 5061 sowie den 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 (1 match)
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (31 matches)
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 (15 matches)
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (5 matches)
    50 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (227 matches)
    60 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (257 matches)
    70 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (130 matches)
    80 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (175 matches)
    90 deny ip any any (5219 matches)
```

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

- **227 SIP**-Pakete am **TCP-Port 5060** für ACE-Leitung 50
- **257 SIP**-Pakete am **TCP-Port 5061** für ACE-Leitung 60
- **130 SIP**-Pakete am **UDP-Port 5060** für ACE-Leitung 70
- **175 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 80

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.

Vorsicht: 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* Typs "show cef", *die* Funktion "show ip interface", "**show cef drop",** die **Funktion "show ip cef switching statistics"** und die Befehle "**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: Der *Befehl* **show** | **Beginnen Sie** *mit dem Befehl regex* und **show** | **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 konfiguriertem Unicast RPF verworfen, weil die Quelladresse der IP-Pakete in der Forwarding Information Base von Cisco Express Forwarding 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, 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 (54955 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .082 .531 .375 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .009 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  167 active, 3929 inactive, 32741 added
  607632 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW            109      0.0         3    40      0.0       0.0      15.4
TCP-BGP          28425      0.0         1    68      0.0       2.9      15.4
TCP-other         1111      0.0         6    40      0.0       0.0      15.4
UDP-NTP           2221      0.0         1    76      0.0       0.0      15.6
UDP-TFTP            95      0.0         4    28      0.0       0.0      15.6
UDP-other          589      0.0         6    28      0.0       0.0      15.4
ICMP                24      0.0        31  1009      0.0      19.9      15.4
Total:           32574      0.0         1    75      0.0       2.5      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.68.44   Et0/1         192.168.60.212  06 F208 098B     4
Et0/0         192.168.38.121  Et0/1         192.168.60.6    06 A826 01BB     3
Et0/0         192.168.224.241 Et0/1         192.168.60.182  06 7536 13C5     5
Et0/0         192.168.212.211 Et0/1         192.168.60.114  06 AB5E 01BB     2
Et0/0         192.168.205.69  Et0/1         192.168.60.110  06 98A5 0ABC    10
Et0/0         192.168.40.45   Et0/1         192.168.60.42   06 5FA7 01BB     2
Et0/0         192.168.4.192   Et0/1         192.168.93.248  11 FFFE 8002    15
Et0/0         192.168.44.66   Et0/1         192.168.178.29  06 A30D 0F4A     3
Et0/0         192.168.36.239  Et0/1         192.168.60.214  11 BCA3 0045     3
Et0/0         192.168.60.164  Et0/1         192.168.60.26   11 1EFB 13C4     2
Et0/0         192.168.234.206 Et0/1         192.168.147.20  11 C959 9972    17
Et0/0         192.168.148.143 Et0/1         192.168.60.25   11 CD48 0045     2
Et0/0         192.168.250.187 Et0/1         192.168.60.41   06 C5B3 098B     3
Et0/0         192.168.227.167 Et0/1         192.168.125.75  06 1048 23FC     3
Et0/0         192.168.107.126 Et0/1         192.168.194.53  06 3767 139B    13
Et0/0         192.168.1.194   Et0/0         192.168.60.155  06 CE95 098B   192
Et0/0         192.168.118.14  Et0/1         192.168.226.46  11 3966 FF31     8
Et0/0         192.168.35.154  Et0/1         192.168.60.77   06 3C5C 0ABC     1
Et0/0         192.168.145.167 Et0/1         192.168.60.74   11 B06D 0045     7
```

```
Et0/0        192.168.56.109  Et0/1         192.168.247.33  11 3F4C 9E2C     6
Et0/0        192.168.28.223  Et0/1         192.168.60.154  06 B35D 13C4     1
Et0/0        192.168.139.201 Et0/1         192.168.60.229  06 8E56 07D0     2
Et0/0        192.168.60.199  Et0/1         192.168.60.242  11 37AF 13C4     5
Et0/0        192.168.212.244 Et0/1         192.168.59.244  06 9CB9 95F7    12
Et0/0        192.168.133.250 Et0/1         192.168.60.49   06 41A2 098B     4
Et0/0        192.168.92.118  Et0/1         192.168.13.136  11 82E2 95B8     2
Et0/0        192.168.206.122 Et0/1         192.168.54.12   06 A09B 7514    11
Et0/0        192.168.164.86  Et0/1         192.168.60.44   11 4ED8 0045     7
Et0/0        192.168.144.222 Et0/1         192.168.60.188  06 770C 13C4     1
Et0/0        192.168.138.85  Et0/1         192.168.60.38   11 9B7D 13C4    11
Et0/0        192.168.185.139 Et0/1         192.168.97.208  11 A25E FE8C     8
Et0/0        192.168.78.45   Et0/1         192.168.92.184  11 08B5 BD08    13
Et0/0        192.168.2.81    Et0/1         192.168.60.138  11 3258 13C5     2
Et0/0        192.168.144.96  Et0/1         192.168.99.50   06 9D6D 4E7E    15
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für SIP auf TCP-Ports (Protokoll-Hex-Wert 06) 5060 (Hex-Wert 13C4) und 5061 (Hex-Wert 13C5) und UDP (Protokoll-Hex-Wert 11) Ports **5060 (Hex-Wert 13C4)** und **5061 (Hexadezimalwert 13C5)**.

Ein Teil dieses Datenverkehrs 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 SIP-Datenverkehr zu vergleichen, der über die TCP-Ports 5060 und 5061 sowie die UDP-Ports 5060 und 5061 gesendet wird. Außerdem sollten die Datenflüsse untersucht werden, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.

Um nur die Datenverkehrsflüsse für SIP-Pakete anzuzeigen, verwenden Sie die TCP-Ports 5060 (Hex-Wert 13C4) und 5061 (Hex-Wert 13C5) und UDP (Protocol Hex-Wert 11) 5060 (Hex-Wert 13C4) und 5061 (Hex value 13C5), **zeigen** die Befehle **den IP-Cache-Fluss | Srclf|**_*06_.*(13C4|13C5)* **einschließen** und **IP-Cache-Fluss anzeigen | include Srclf**|_*11_.*(13C4|13C5)* zeigt die zugehörigen TCP- und UDP-NetFlow-Datensätze wie folgt an:

TCP-Flows

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

UDP-Datenflüsse

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.151.1   Et0/1          192.168.60.96   11 2C2D 13C5     3
Et0/0         192.168.237.123 Et0/1          192.168.60.131  11 5712 13C5     4
Et0/0         192.168.246.100 Et0/1          192.168.60.37   11 FCBC 13C5     4
```

```
Et0/0          192.168.126.21  Et0/1          192.168.60.103  11 9716 13C4     1
Et0/0          192.168.60.28   Et0/1          192.168.60.244  11 E40B 13C4   192
Et0/0          192.168.56.139  Et0/1          192.168.60.218  11 4EE8 13C4    10
Et0/0          192.168.51.212  Et0/1          192.168.60.209  11 835D 13C4     3
Et0/0          192.168.252.73  Et0/1          192.168.60.115  11 521E 13C4     3
router#
```

Cisco ASA 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-Pakete an den TCP-Ports 5060 und 5061 sowie den UDP-Ports 5060 und 5061, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen Geräten verwendet wird. 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 in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-
Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 ! !-- The following vulnerability-specific access control
entries !-- (ACEs) can aid in identification of attacks ! access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy
extended deny udp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy
extended deny udp any 192.168.60.0 255.255.255.0 eq 5061 ! !-- Permit or deny all
other Layer 3 and Layer 4 traffic in accordance !-- with existing security policies
and configurations ! !-- Explicit deny for all other IP traffic ! access-list tACL-
Policy extended deny ip any any ! !-- Apply tACL to interface(s) in the ingress
direction ! access-group tACL-Policy in interface outside
```

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.

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 den TCP-Ports 5060 und 5061 sowie den 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=224)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=28)
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq sip (hitcnt=36)
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=41)
access-list tACL-Policy line 5 extended deny tcp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=78)
access-list tACL-Policy line 6 extended deny tcp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=39)
access-list tACL-Policy line 7 extended deny udp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=437)
access-list tACL-Policy line 8 extended deny udp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=478)
access-list tACL-Policy line 9 extended deny ip any any (hitcnt=563)
firewall#
```

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

- **78 SIP**-Pakete am **TCP-Port 5060 (SIP)** für ACE-Leitung 5
- **39 SIP**-Pakete am **TCP-Port 5061** für ACE-Leitung 6
- **437 SIP**-Pakete auf **UDP-Port 5060 (SIP)** für ACE-Leitung 7
- **478 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 8

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

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

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

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

Im vorherigen Beispiel zeigen die für die tACL-*tACL-Richtlinie* protokollierten Meldungen potenziell gefälschte **SIP-**Pakete für die **TCP-Ports 5060 und 5061** sowie die **UDP-Ports 5060 und 5061 an,** die an den betroffenen Geräten zugewiesen 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 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.202 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.126 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.22 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.75 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.248 to 192.168.60.1 on interface outside
```

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 (rpf-violated)                    10
```

Im vorherigen Beispiel hat Unicast RPF **10 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.

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, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Diese Schwachstellen können durch die folgenden Signaturen entdeckt werden:

- 29219-0 CUCM-Meldung "DoS" für fehlerhafte Registrierung
- 29239-0 Sicherheitslücke in Cisco CUP-Arbeitsspeicher

29219-0 CUCM-Meldung "DoS" für fehlerhafte Registrierung

Beginnend mit dem Signatur-Update S510 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, kann diese Schwachstelle mit der Signatur 29219/0 erkannt werden (Signature Name: CUCM Malformed REGISTER Message DoS). Signatur 29219/0 ist standardmäßig aktiviert, löst ein Ereignis mit *mittlerem* Schweregrad aus, hat eine Signaturtreue-Bewertung (SFR) von 90 und wird mit der Standardereignisaktion **"create-alert"** konfiguriert.

Diese Signatur wird ausgelöst, wenn eine falsch formatierte SIP REGISTER-Nachricht erkannt wird, die in Cisco Unified Communications Manager einen 'Denial of Service' verursachen kann. Die Schwachstelle ist in der Cisco Bug-ID CSCtf66305 dokumentiert und der CVE-Kennung CVE-2010-2838 zugewiesen. Das Auslösen dieser Signatur kann auf einen potenziellen Exploit dieser Schwachstelle hinweisen.

29239-0 Sicherheitslücke in Cisco CUP-Arbeitsspeicher

Beginnend mit dem Signatur-Update S510 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, kann diese Schwachstelle mit der Signatur 29239/0 erkannt werden (Signature Name: Cisco CUP Memory Corruption Vulnerability). Signatur 29239/0 ist standardmäßig aktiviert, löst ein Ereignis *mit hohem* Schweregrad aus, hat eine Signaturtreue-Bewertung (SFR) von 90 und wird mit der Standardereignisaktion **"create-alert"** konfiguriert.

Diese Signatur wird bei Versuchen ausgelöst, einen Fehler bei der Speicherbeschädigung im Cisco CUP über den TCP-Port 5070 auszunutzen. Die Schwachstelle ist in der Cisco Bug-ID CSCtd39629 dokumentiert und wurde mit der CVE-Kennung CVE-2010-2840 versehen. Das Auslösen dieser Signatur kann auf einen potenziellen Exploit dieser Schwachstelle 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.

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 werden die IPS-Signaturen 29219-0 (Signature Name: CUCM Malformed REGISTER Message DoS) und 29239-0 (Signature Name: Cisco CUP Memory Corruption Vulnerability) verwendet. Nach dem Download des dynamischen Signatur-Updates für S510 wird mithilfe der Schlüsselwörter **NR-29219/0** für die IPS-Signatur 29219/0 und **NR-29239/0** für die IPS-Signatur 29239/0 und des Abfragetyps **Alle übereinstimmenden Ereignis-Rohmeldungen** auf der Cisco Security MARS-Appliance ein Bericht mit den durch die IPS-Signatur erstellten Vorfällen bereitgestellt.

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

Revisionsverlauf

Version 1.0	25. August 2010	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
- Überblick über die XSS-Bedrohungsvektoren (Cross-Site Scripting)
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- NetFlow-Leistungsanalyse
- Cisco Network Foundation Protection - Whitepaper
- Cisco Network Foundation Protection - Präsentationen
- Erkennung von und Beseitigung von TTL-Ablaufangriffen
- Ein sicherheitsorientierter Ansatz für die IP-Adressierung
- Gegenmaßnahmen für die böswillige Verwendung von IPv6-Typ-0-Routing-Headern
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- 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.