Identifizieren und Beheben der verschiedenen Sicherheitslücken in Cisco Unified Communications Manager

Identifizieren und Beheben der verschiedenen Sicherheitslücken in Cisco Unified Communications Manager

Beratungs-ID: cisco-amb-20110427-cucm

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

Version 1.1

Zur öffentlichen Veröffentlichung 2011 April 27 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zur PSIRT-Sicherheitsempfehlung für *mehrere Schwachstellen in Cisco Unified Communications Manager* und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

Merkmale der Schwachstelle

Cisco Unified Communications Manager weist mehrere Schwachstellen auf. Die folgenden Unterabschnitte fassen diese Schwachstellen zusammen:

Session Initiation Protocol (SIP) Denial of Service-Schwachstellen: Diese Schwachstellen können ohne Authentifizierung und ohne Eingreifen der Endbenutzer per Remote-Zugriff ausgenutzt werden. Wenn diese Schwachstellen erfolgreich ausgenutzt werden, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen.

Die Angriffsvektoren zur Ausnutzung werden durch 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-2011-1604, CVE-2011-1605 und CVE-2011-1606 zugewiesen.

Unautorisierte Datei-Upload-Schwachstelle von Cisco Unified Reporting: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann ein Angreifer von einem entfernten Standort aus eine schädliche Datei hochladen. Der Angriffsvektor für die Ausnutzung erfolgt über HTTPS-Pakete mit dem TCP-Port 8443.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-1607 zugewiesen.

Mehrere Schwachstellen durch SQL Injection: Diese Schwachstellen können per Fernzugriff mit und ohne Authentifizierung und ohne Endbenutzer-Interaktion ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstellen kann die Offenlegung von Informationen ermöglichen, sodass ein Angreifer Informationen über das betroffene Gerät erhalten kann.

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

- HTTP über TCP-Port 80
- HTTPS mit TCP-Port 443
- HTTP über TCP-Port 8080
- HTTPS mit TCP-Port 8443

Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2011-1609 und CVE-2011-1610 zugewiesen.

Informationen zu anfälliger, nicht betroffener und fest installierter Software finden Sie in der PSIRT-Sicherheitsberatung, die unter folgendem Link verfügbar ist: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110427-cucm.

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.

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- und UDP-Ports 5060 und 5061, HTTP-Pakete an den TCP-Ports 80 und 8080 und HTTPS-Pakete an den TCP-Ports 443 und 8443, 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 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 80 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 443 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 ! !--
The following vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
5060 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny
udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny udp any 192.168.60.0
0.0.0.255 eq 5061 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80 access-
list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 8080 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
8443 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !--
with existing security policies and configurations ! !-- Explicit deny for all other
IP traffic ! access-list 150 deny ip any any ! !-- Apply tACL to interfaces in the
ingress direction ! interface GigabitEthernet0/0 ip access-group 150 in
```

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- und UDP-Ports 5060 und 5061, die

HTTP-Pakete an den TCP-Ports 80 und 8080 und die HTTPS-Pakete an den TCP-Ports 443 und 8443, 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 80
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
    90 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (17 matches)
    100 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (19 matches)
    110 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (3 matches)
    120 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (49 matches)
    130 deny tcp any 192.168.60.0 0.0.0.255 eq 80 (32 matches)
    140 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (20 matches)
    150 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (35 matches)
    160 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (10 matches)
    170 deny ip any any
router#
```

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

- **17 SIP**-Pakete am **TCP-Port 5060** für ACE-Leitung 90
- **19 SIP**-Pakete am **TCP-Port 5061** für ACE-Leitung 100
- **3 SIP**-Pakete am **UDP-Port 5060** für ACE-Leitung 110
- **49 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 120
- **32 HTTP-**Pakete an **TCP-Port 80** für ACE-Leitung 130
- **20 HTTPS**-Pakete auf **TCP-Port 443** für ACE-Leitung 140
- **35 HTTP-**Pakete an **TCP-Port 8080** für ACE-Leitung 150
- **10 HTTPS**-Pakete auf **TCP-Port 8443** für ACE-Leitung 160

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 *internen Steckplatz/Port des* Schnittstellentyps "show cef", die **show ip interface,** die **show cef drop-Funktion**, 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 |** *Regex* **starten** und *Befehl* **anzeigen | 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 (31715553 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .005 .175 .632 .032 .095 .003 .003 .003 .002 .000 .005 .002 .000 .000 .000

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

IP Flow Switching Cache, 4456704 bytes
  24 active, 65512 inactive, 5451612 added
  557541771 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet         811      0.0       137    41      0.0      32.3      16.4
TCP-FTP           2108      0.0         6    44      0.0       0.5      22.1
TCP-FTPD             5      0.0        13    52      0.0       0.7       1.5
TCP-WWW         133468      0.0         4   223      0.1       5.5      50.9
TCP-SMTP         32583      0.0         5    60      0.0      28.3      60.0
TCP-other       627608      0.1        12   175      1.8      57.8      24.1
UDP-DNS         284078      0.0         3    63      0.2      15.1      53.5
UDP-NTP          94456      0.0         1    76      0.0       0.3      60.5
UDP-Frag             1      0.0         9  1260      0.0       0.4      60.2
UDP-other      1102669      0.2         8   102      2.1      34.3      47.5
```

```
ICMP          1980458      0.4         2    89      1.1      14.3      58.5
IGMP           469264      0.1         2    37      0.2      58.2      41.0
IPINIP              2      0.0         1    76      0.0       0.0      60.4
IPv6INIP            3      0.0         1   863      0.0       0.0      60.4
GRE                 2      0.0         1   697      0.0       0.0      60.4
IP-other       724037      0.1         9    89      1.5      95.0      15.6
Total:        5451553      1.2         5   113      7.3      37.5      44.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  11 0984 00A1     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  11 0911 13C5     3
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   11 0B3E 13C4     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 13C4     1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
Gi0/0         192.168.120.20  Gi0/1         192.168.60.102  06 0984 1F90     1
Gi0/0         192.168.12.45   Gi0/1         192.168.60.138  06 0911 13C5     3
Gi0/1         192.168.150.41  Gi0/0         192.168.60.24   06 0016 12CA     1
Gi0/0         192.168.12.87   Gi0/1         192.168.60.28   06 0B3E 0050     5
Gi0/0         192.168.10.12   Gi0/1         192.168.60.97   06 0B89 01BB     1
Gi0/0         10.88.226.8     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.15   Gi0/1         192.168.60.209  06 0BD7 20FB     1
Gi0/0         10.89.16.216    Gi0/1         192.168.150.8   06 12CA 0016     1
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für SIP an den TCP-Ports 5060 (Hexadezimalwert 13C4) und 5061 (Hexadezimalwert 13C5) und den UDP-Ports 5060 (Hexadezimalwert 13C4) und 5061 (Hexadezimalwert 13C5 und HTTP auf den TCP-Ports 80 (Hexadezimalwert 0050) und 8080 (Hexadezimalwert 1F90) und HTTPS auf den TCP-Ports 443 (Hexadezimalwert 01BB) und 8443 (Hexadezimalwert 20FB).

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-Datenverkehr zu vergleichen, der über UDP-Port 5060 und Port 5061 gesendet wird. Außerdem sollten sie die Datenflüsse untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.

Um nur die Datenverkehrsflüsse für SIP-Pakete auf den UDP-Ports 5060 (Hexadezimalwert 13C4) und 5061 (Hexadezimalwert 13C5) anzuzeigen, muss der Befehl **ip cache flow anzeigen. | 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         192.168.12.110  Gi0/1         192.168.60.163  11 092A 13C4     6
Gi0/0         192.168.11.230  Gi0/1         192.168.60.20   11 0C09 13C4     1
Gi0/0         192.168.11.131  Gi0/1         192.168.60.245  11 0B66 13C5    18
Gi0/0         192.168.13.7    Gi0/1         192.168.60.162  11 0914 13C4     1
router#
```

Nur die Datenverkehrsflüsse für SIP-Pakete auf den TCP-Ports 5060 (Hexadezimalwert 13C4) und 5061 (Hexadezimalwert 13C5) und HTTP-Pakete auf den TCP-Ports 80 (Hexadezimalwert 0050) und 8080 (Hexadezimalwert 1F90) und HTTPS-Pakete auf den TCP-Ports 44 anzeigen 3 (Hexadezimalwert 01BB) und 8443 (Hexadezimalwert 20FB). Der Befehl **zeigt den IP-Cache-Fluss**

an. | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB) zeigt die zugehörigen TCP-NetFlow-Datensätze wie folgt an:

TCP-Flows

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB)
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.12.110   Gi0/1         192.168.60.163  06 092A 13C5     6
Gi0/0         192.168.11.230   Gi0/1         192.168.60.20   06 0C09 0050     1
Gi0/0         192.168.11.131   Gi0/1         192.168.60.245  06 0B66 01BB    18
Gi0/0         192.168.13.7     Gi0/1         192.168.60.162  06 0914 0050     7
Gi0/0         192.168.241.106  Gi0/1         192.168.60.27   06 0B7B 13C4    12
Gi0/0         192.168.19.222   Gi0/1         192.168.60.120  06 0C09 20FB    16
Gi0/0         192.168.12.121   Gi0/1         192.168.60.245  06 0B66 01BB    19
Gi0/0         192.168.14.17    Gi0/1         192.168.60.183  06 0914 1F90     9
Gi0/0         192.168.41.86    Gi0/1         192.168.60.217  06 0B7B 20FB     2
router#
```

Cisco ASA 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- und UDP-Ports 5060 und 5061, HTTP-Pakete an den TCP-Ports 80 und 8080 und HTTPS-Pakete an den TCP-Ports 443 und 8443, 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 sip access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-
Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq sip
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8080 access-list tACL-
```

```
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 ! !-
- The following vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny udp any
192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended deny udp any
192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq www access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 ! !-- Permit or deny all other Layer 3 and Layer 4
traffic in accordance !-- with existing security policies and configurations ! !--
Explicit deny for all other IP traffic ! access-list tACL-Policy extended deny ip any
any ! !-- Apply tACL to interface(s) in the ingress direction ! access-group tACL-
Policy in interface outside
```

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 an den TCP- und UDP-Ports 5060 und 5061, die HTTP-Pakete an den TCP-Ports 80 und 8080 und die HTTPS-Pakete an den TCP-Ports 443 und 8443 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; 17 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq www
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1 192.168.60.0
```

```
255.255.255.0 eq https
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8443
access-list tACL-Policy line 9 extended deny tcp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=30)
access-list tACL-Policy line 10 extended deny tcp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=43)
access-list tACL-Policy line 11 extended deny udp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=70)
access-list tACL-Policy line 12 extended deny udp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=14)
access-list tACL-Policy line 13 extended deny tcp any 192.168.60.0 255.255.255.0 eq
www (hitcnt=45)
access-list tACL-Policy line 14 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=53)
access-list tACL-Policy line 15 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8080 (hitcnt=70)
access-list tACL-Policy line 16 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8443 (hitcnt=61)
access-list tACL-Policy line 17 extended deny tcp any any
```

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

- **30 SIP**-Pakete am **TCP-Port 5060** für ACE-Leitung 9
- **43 SIP**-Pakete am **TCP-Port 5061** für ACE-Leitung 10
- **70 SIP**-Pakete am **UDP-Port 5060** für ACE-Leitung 11
- **14 SIP**-Pakete am **UDP-Port 5061** für ACE-Leitung 12
- **45 HTTP**-Pakete an **TCP-Port 80** für ACE-Leitung 13
- **53 HTTPS**-Pakete auf **TCP-Port 443** für ACE-Leitung 14
- **70 HTTP**-Pakete am **TCP-Port 8080** für ACE-Leitung 15
- **61 HTTPS**-Pakete am **TCP-Port 8443** für ACE-Leitung 16

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
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.18/16784
         dst inside:192.168.60.191/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.200/16785
         dst inside:192.168.60.33/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.99/16786
         dst inside:192.168.60.240/5061 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.100/16787
         dst inside:192.168.60.115/5061 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.88/18683
         dst inside:192.168.60.38/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.175/18684
         dst inside:192.168.60.250/5061 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-*tACL-Richtlinie* protokollierten Nachrichten potenziell gefälschte **SIP-**Pakete für die **TCP-** und **UDP-Ports 5060 und 5061 an,** die an den Adressblock gesendet wurden, der den betroffenen Geräten zugewiesen ist.

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
  Apr 27 2011 00:03:42: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %ASA-1-106021: Deny TCP reverse path check from
```

```
        192.168.60.1 to 192.168.60.100 on interface outside
```

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.

Cisco Intrusion Prevention System

Eindämmung: Cisco IPS-Signaturereignisaktionen

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

- 35846-0 - Cisco CUCM-Remote-Codeausführung
- 35866-0 - Sicherheitslücke in Cisco CUCM-SIP
- 35085-0 - Cisco Call Manager SQL-Injection

35846-0 - Cisco CUCM-Remote-Codeausführung

Ab dem Signatur-Update S562 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 35846/0 (Signature Name: Cisco CUCM Remote Code Execution) erkannt werden. Signatur 35846/0 ist standardmäßig aktiviert, löst ein Ereignis *mit hohem* Schweregrad aus, hat eine Signaturtreue-Bewertung (SFR) von 95 und wird mit der Standardereignisaktion **"create-alert"** konfiguriert.

Signatur 35846/0 wird ausgelöst, wenn ein einzelnes Paket erkannt wird, das über den SIP-Port 5060 gesendet wurde. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

35866-0 - Sicherheitslücke in Cisco CUCM-SIP

Ab dem Signatur-Update S562 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 35866/0 erkannt werden (Signature Name: Cisco CUCM SIP Vulnerability). Signatur 35866/0 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.

Signatur 35866/0 wird ausgelöst, wenn ein einzelnes Paket erkannt wird, das über den SIP-Port 5060 gesendet wurde. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

35085-0 - Cisco Call Manager SQL-Injection

Beginnend mit dem Signatur-Update S562 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, können diese Schwachstellen mit der Signatur 35085/0 (Signature Name: Cisco Call Manager SQL Injection) erkannt werden. Signatur 35085/0 ist standardmäßig aktiviert, löst ein Ereignis *mit hohem* Schweregrad aus, hat eine Signaturtreue-Bewertung (SFR) von 85 und wird mit der Standardereignisaktion **"create-alert"** konfiguriert.

Signatur 35085/0 wird ausgelöst, wenn ein SQL-Injection-Angriff auf den Cisco Call Manager erkannt wird. 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 35846/0 (Signaturname: Cisco CUCM Remote Code Execution), IPS-Signatur 35866/0 (Signaturname: Cisco CUCM SIP Vulnerability) und die IPS-Signatur 35085/0 (Signaturname: Cisco Call Manager SQL Injection) verwendet. Nach dem Download des dynamischen Signatur-Updates für S562 wird ein Bericht mit dem Schlüsselwort **NR-35846/0** für die IPS-Signatur 35846/0, dem Schlüsselwort **NR-35866/0** für die IPS-Signatur 35866/0 oder dem Schlüsselwort **NR-35085/0** für die IPS-Signatur 35085/0 und dem Abfragetyp **Alle übereinstimmenden Ereignisse** auf der Cisco Security MARS-Appliance bereitgestellt. von der IPS-Signatur erstellt.

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	27. APRIL 2011	Aktualisiert, um Informationen zu IPS-Signaturen und Cisco Security MARS einzuschließen.
Version 1.0	27. APRIL 2011	Erste 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 Network Foundation Protection - Präsentationen
- Ein sicherheitsorientierter Ansatz für die IP-Adressierung
- 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.