Identifizierung und Beseitigung der Schwachstellen bei Cisco Unified Communications Manager und Presence Server

Identifizierung und Beseitigung der Schwachstellen bei Cisco Unified Communications Manager und Presence Server

Beratungs-ID: cisco-amb-20070711-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070711-cucm

Version 1.0

Zur öffentlichen Veröffentlichung 2007 11. Juli 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zu den folgenden PSIRT-Sicherheitsempfehlungen: *Überlaufschwachstellen von Cisco Unified Communications Manager* und *Sicherheitslücken bei nicht autorisiertem Zugriff von Cisco Unified Communications Manager und Presence Server* sowie Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

Merkmale der Schwachstelle

Cisco Unified Communications Manager und Cisco Unified Presence Server weisen mehrere Schwachstellen auf. Diese Schwachstellen werden in den folgenden Unterabschnitten zusammengefasst:

Certificate Trust List Provider Service Overflow: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser

Schwachstelle kann die Ausführung von beliebigem Code ermöglichen oder eine Denial of Service (DoS)-Bedingung verursachen. Der Angriffsvektor besteht aus Paketen, die an den Service-Port des CTL-Anbieters (Certificate Trust List) gesendet werden. Der Standardport ist der TCP-Port 2444. Administratoren können den vom CTL Provider-Service verwendeten Port überprüfen, indem Sie die Benutzeroberfläche von Cisco Unified Communications Manager aufrufen: Wählen Sie **System > Service Parameters (System > Dienstparameter)**. Wählen Sie den Server aus der Dropdown-Liste aus. Wählen Sie dann **Cisco CTL Provider (Inaktiv)** oder **Cisco CTL Provider (Aktiv)** aus der Dropdown-Liste Service aus. Der Begriff *(Inaktiv)* oder *(Aktiv)*, der an den Dienstnamen in dieser Liste angehängt wird, gibt an, ob der Dienst aktiviert ist. Nachdem der Dienst ausgewählt wurde, wird der Parameter für die Portnummer im Bereich unter den Dropdown-Listen Server und Dienst angezeigt. Der Wert für diesen Parameter gibt den Port an, der für den aktiven Service verwendet wird. Zum Zeitpunkt der Veröffentlichung war keine CVE-ID mit dieser Schwachstelle verbunden.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie im PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Real-Time Information Server Data Collector Heap Overflow: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff aus der Ferne ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen oder eine Denial of Service (DoS)-Bedingung verursachen. Der Angriffsvektor besteht aus Paketen, die an den Datensammlungsport des Real-Time Information Server (RIS) gesendet werden. Der Standardport ist der TCP-Port 2556. Administratoren können den vom RIS Data Collector-Service verwendeten Port überprüfen, indem sie die Benutzeroberfläche von Cisco Unified Communications Manager aufrufen: Wählen Sie **System > Service Parameters (System > Service-Parameter)**. Wählen Sie den Server aus der Dropdown-Liste aus. Wählen Sie dann **Cisco RIS Data Collector (Inaktiv)** oder **Cisco RIS Data Collector (Aktiv)** aus der Dropdown-Liste Service aus. Der Begriff *(Inaktiv)* oder *(Aktiv)*, der an den Dienstnamen in dieser Liste angehängt wird, gibt an, ob der Dienst aktiviert ist. Nachdem der Dienst ausgewählt wurde, wird der RIS-Cluster-TCP-Port-Parameter im Bereich für clusterweite Parameter angezeigt. Der Wert für diesen Parameter gibt den Port an, der für den aktiven Service verwendet wird. Zum Zeitpunkt der Veröffentlichung war keine CVE-ID mit dieser Schwachstelle verbunden.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie im PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Nicht autorisierter Administrator kann Cisco Unified Communications Manager/Cisco Unified Presence Server System-Services aktivieren/beenden: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriffe remote ausgenutzt werden. Bei einer erfolgreichen Nutzung können nicht autorisierte Cisco Unified Communications Manager-/Cisco Unified Presence Server-Administratoren Systemdienste in einer Cluster-Umgebung aktivieren oder beenden. Dadurch können wichtige Sprachdienste unterbrochen oder angehalten werden. Der Angriffsvektor ist das SSL-Protokoll, das Pakete des TCP-Ports 8443 verwendet. Weitere Informationen zu den von der betroffenen Software verwendeten Ports finden Sie unter Cisco CallManager TCP und UDP Port Usage. Zum Zeitpunkt der Veröffentlichung war keine CVE-ID mit dieser Schwachstelle verbunden.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie im PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Nicht autorisierter Administrator kann Cisco Unified Communications Manager/Cisco Unified Presence Server SNMP-Einstellungen anzeigen: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff aus der Ferne ausgenutzt werden. Bei einer erfolgreichen Nutzung kann ein nicht autorisierter Administrator die SNMP-Einstellungsansicht auf der Verwaltungsoberfläche eines Cisco Unified Communications Manager-/Cisco Unified Presence Server-Clusterknotens durchsuchen. Der Angriffsvektor ist das SSL-Protokoll, das Pakete des TCP-Ports 8443 verwendet. Weitere Informationen zu den von der betroffenen Software verwendeten Ports finden Sie unter Cisco CallManager TCP und UDP Port Usage. Zum Zeitpunkt der Veröffentlichung war keine CVE-ID mit dieser Schwachstelle verbunden.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie im PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Überblick über die Risikominderungstechnik

Cisco Geräte bieten eine Reihe von Gegenmaßnahmen für die in diesem Dokument beschriebenen Schwachstellen. Den Administratoren wird empfohlen, viele dieser Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs im Netzwerk zu betrachten.

Die Cisco IOS Software bietet mithilfe von Transit-Zugriffskontrolllisten (tACLs) effektive Möglichkeiten zur Verhinderung von Exploits.

Cisco Adaptive Security Appliances der Serie ASA 5500, Cisco Security Appliances der Serie PIX 500 und das Firewall Services Module (FWSM) für Cisco Catalyst Switches der Serie 6500 sowie Cisco Router der Serie 7600 bieten ebenfalls effektiven Exploit-Schutz mithilfe von Transit-Zugriffskontrolllisten (tACLs).

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, die in diesem Dokument beschriebenen Schwachstellen auszunutzen.

Cisco IOS NetFlow kann mithilfe von Flow Records Einblick in Exploit-Versuche gewähren. Cisco IOS Software, Cisco ASA, Cisco PIX Security Appliances und FWSM-Firewalls bieten Transparenz durch Syslog-Meldungen und die Zählerwerte, die in der Ausgabe der **show-**Befehle angezeigt werden.

Risikomanagement

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

Gerätespezifische Eindämmung und Identifizierung

Vorsicht: Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab.

Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

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

- Cisco IOS-Router und -Switches
- Cisco IOS-NetFlow
- Cisco ASA, PIX und FWSM-Firewalls

Cisco IOS-Router und -Switches

Eindämmung: Transit-Zugriffskontrolllisten

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

Die tACL-Richtlinie verweigert nicht autorisierte Pakete für den CTL-Anbieterdienst auf dem TCP-Port 2444, den RIS Data Collector auf dem TCP-Port 2556 und die Cisco Unified Communications Manager-/Cisco Unified Presence Server-Systemdienste auf dem TCP-Port 8443, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.1.0/24 der von den betroffenen Geräten verwendete IP-Adressraum des Netzwerks, und der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie unter Transit Access Control Lists: Filtering at Your Edge.

```
!-- Include any explicit permit statements for trusted sources !-- that require
access on the vulnerable port(s) ! access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2444 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2556 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 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 192.168.1.0 0.0.0.255 eq 2444 access-list 150 deny tcp any 192.168.1.0
0.0.0.255 eq 2556 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 ! !--
Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list 150 deny ip any any ! !-- Apply tACL to interface(s) 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. Dies könnte den unerwünschten Effekt einer erhöhten CPU-Auslastung haben, da das Gerät diese

"ICMP unreachable"-Meldungen generieren muss. 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 icmp unreachables** deaktiviert werden. Die Durchsatzbegrenzung "ICMP unreachable" kann mithilfe des globalen Konfigurationsbefehls **ip icmp rate-limit unreachable** *interval-in-ms* vom Standardwert geändert werden.

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem der Administrator die tACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der CTL Provider-Service-Pakete an den TCP-Ports 2444, der RIS Data Collector-Pakete am TCP-Port 2556 und der CUCM/CUPS System-Service-Pakete am TCP-Port 8443, die gefiltert wurden. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show ip access-lists 150**:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444 (2 matches)
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556 (3 matches)
    30 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443 (3 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 2444 (3 matches)
    50 deny tcp any 192.168.1.0 0.0.0.255 eq 2556 (4 matches)
    60 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 (5 matches)
    70 deny ip any any
router#
```

Im vorherigen Beispiel hat die Zugriffsliste 150 **3 Pakete auf dem TCP-Port 2444** für die ACE-Sequenz-ID 40, **4 Pakete auf dem TCP-Port 2556** für die ACE-Sequenz-ID 50 und **5 Pakete auf dem TCP-Port 8443** für die ACE-Sequenz-ID 60 verworfen.

Identifizierung: Protokollierung der Zugriffsliste

Die ACL-Option **log** oder **log-input** führt dazu, 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. Der Einfluss der ACL-Protokollierung auf die CPU wird von zwei Faktoren bestimmt: Prozess-Switching als Ergebnis von Paketen, die mit protokollfähigen ACEs übereinstimmen, sowie Protokollgenerierung und -übertragung.

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

Weitere Informationen zur Konfiguration und Verwendung der ACL-Protokollierung finden Sie im Whitepaper "Applied Intelligence" unter http://www.cisco.com/web/about/security/intelligence/acl-logging.html.

Cisco IOS-NetFlow

Identifizierung: Identifikation des Datenverkehrsflusses mithilfe von NetFlow-Datensätzen

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

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

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

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.201 Gi0/1         192.168.1.102   06 0984 098C     1
Gi0/0         192.168.100.5   Gi0/1         192.168.1.158   06 0911 09FC     3
Gi0/0         192.168.105.60  Gi0/1         192.89.1.226    06 0016 12CA     1
Gi0/0         192.168.105.97  Gi0/1         192.168.1.28    06 0B3E 098C     5
Gi0/0         192.168.105.197 Gi0/1         192.168.1.248   06 0B3E 20FB     7
Gi0/0         192.168.1.17    Gi0/1         192.168.1.97    11 0B89 00A1     1
Gi0/0         192.168.105.7   Gi0/1         192.168.1.8     06 0B3E 20FB     4
Gi0/1         10.88.226.1     Gi0/0         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.1.239   06 0E8A 09FC     1
Gi0/1         10.89.16.226    Gi0/0         192.168.150.60  06 12CA 0901     1
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für den CTL Provider-Dienst am **TCP-Port**

2444 (Hexadezimalwert 098C), den RIS Data Collector am **TCP-Port 2556 (Hexadezimalwert 09FC)** und den Cisco Unified Communications Manager/Cisco Unified Presence Server System Service am **TCP-Port 8443 (10). Hexadezimalwert 20 FB)**. Administratoren sollten diese Datenflüsse mit der Basisauslastung für den Datenverkehr vergleichen, der über die TCP-Ports 2444, 2556 und 8443 gesendet wird. Außerdem sollten sie die Flüsse untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.

Um nur die Datenverkehrsflüsse für Pakete auf dem TCP-Port 2444 (Hexadezimalwert 098C), Pakete auf dem TCP-Port 2556 (Hexadezimalwert 09FC) oder Pakete auf dem TCP-Port 8443 (Hexadezimalwert 20FB) anzuzeigen, **zeigt** der Befehl den **IP-Cache-Fluss | include SrcIf|_06_.*(098C|09FC|20FB)** zeigt die zugehörigen NetFlow-Datensätze wie folgt an:

```
router#show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.110  Gi0/1         192.168.1.163   06 0E2A 098C     6
Gi0/0         192.168.105.230  Gi0/1         192.168.1.20    06 0C09 098C     1
Gi0/0         192.168.101.131  Gi0/1         192.168.1.245   06 0B66 20FB    18
Gi0/0         192.168.100.7    Gi0/1         192.168.1.162   06 0D14 09FC     1
Gi0/0         192.168.100.86   Gi0/1         192.168.1.27    06 0B7B 09FC     2
router#
```

Cisco ASA, PIX und FWSM-Firewalls

Eindämmung: Transit-Zugriffskontrolllisten

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

Die tACL-Richtlinie verweigert nicht autorisierte CTL Provider-Service-Pakete auf dem TCP-Port 2444, RIS Data Collector-Pakete auf dem TCP-Port 2556 und Cisco Unified Communications Manager/Cisco Unified Presence Server System-Service-Pakete auf dem TCP-Port 8443, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.1.0/24 der von den betroffenen Geräten verwendete IP-Adressraum des Netzwerks, und der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie unter Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include any explicit permit statements for trusted sources !-- that require
access on the vulnerable port(s) ! access-list Transit-ACL-Policy extended permit tcp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2556 access-list
Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq 8443 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
```

```
can aid in identification of attacks ! access-list Transit-ACL-Policy extended deny
tcp any 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy extended
deny tcp any 192.168.1.0 255.255.255.0 eq 2556 access-list Transit-ACL-Policy
extended deny tcp any 192.168.1.0 255.255.255.0 eq 8443 ! !-- Permit/deny all other
Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and
configurations ! !-- Explicit deny for all other IP traffic ! access-list Transit-
ACL-Policy extended deny ip any any ! !-- Apply tACL to interface(s) in the ingress
direction ! access-group Transit-ACL-Policy in interface outside !
```

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der CTL Provider-Service-Pakete auf dem TCP-Port 2444, RIS Data Collector-Pakete auf dem TCP-Port 2556 und Cisco Unified Communications Manager/Cisco Unified Presence Server System-Service-Pakete auf dem TCP-Port 8443 identifizieren, die gefiltert wurden. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show access-list Transit-ACL-Policy**:

```
firewall# show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 7 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2444 (hitcnt=2) 0xaca1615c
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2556 (hitcnt=4) 0x991fbe7d
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 8443 (hitcnt=3) 0xd2687825
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2444 (hitcnt=19) 0xc81a715d
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2556 (hitcnt=11) 0x67db99e7
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.1.0255.255.255.0
            eq 8443 (hitcnt=7) 0xb322498f
access-list Transit-ACL-Policy line 7 extended deny ip any any(hitcnt=0) 0xc797eb99
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste "Transit-ACL-Policy" **19 Pakete für den TCP-Port 2444, 11 Pakete für den TCP-Port 2556** und **7 Pakete für den TCP-Port 8443, die** von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden, verworfen. Darüber hinaus kann die Syslog-Meldung 106023 nützliche Informationen bereitstellen, z. B. die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Port-Nummern sowie das IP-Protokoll für das abgelehnte Paket.

Identifizierung: Firewall Access List, Syslog-Meldungen

Die Firewall-Syslog-Meldung 106023 wird für Pakete generiert, die von einem ACE abgelehnt wurden, der nicht über das **log**-Schlüsselwort verfügt. Weitere Informationen zu dieser Syslog-Meldung finden Sie unter Cisco Security Appliance System Log Message - 106023.

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

Im folgenden Beispiel **zeigt** die **Protokollierung | grep** *regexp* 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 Verwenden der Befehlszeilenschnittstelle.

```
firewall#show logging | grep 106023
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
            inside:192.168.1.191/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 dst
            inside:192.168.1.33/2556 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
            inside:192.168.1.240/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 dst
            inside:192.168.1.115/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
            inside:192.168.1.38/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 dst
            inside:192.168.1.250/2444 by access-group "Transit-ACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-Transit-ACL-Richtlinie protokollierten Nachrichten Pakete für den **TCP-Port 2444,** Pakete für den **TCP-Port 2556** und Pakete für den **TCP-Port 8443 an,** die an den der Netzwerkinfrastruktur zugewiesenen Adressblock gesendet wurden.

Weitere Informationen zu Syslog-Meldungen für ASA- und PIX-Sicherheits-Appliances finden Sie unter Cisco Security Appliance System Log Messages. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie unter Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 Firewall Services Module Logging Configuration (Protokollierungskonfiguration) und System Log Messages (Systemprotokollmeldungen).

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 1.0	11. Juli 2007	Erste öffentliche Veröffentlichung

Cisco Sicherheitsverfahren

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

Zugehörige Informationen

- Cisco Applied Mitigation Bulletins
- Protecting Your Core: Infrastructure Protection - Zugriffskontrolllisten
- Transit-Zugriffskontrolllisten: Filterung am Netzwerk-Edge
- Protokollierung der Zugriffskontrollliste
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Allgemeine Liste der Sicherheitslücken und Risiken

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.