Identifizieren und Eindämmen der Ausnutzung der Denial-of-Service-Schwachstelle des Cisco Content Services Gateway

Identifizieren und Eindämmen der Ausnutzung der Denial-of-Service-Schwachstelle des Cisco Content Services Gateway

Beratungs-ID: cisco-amb-20110706-csg

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110706-csg

Version 1.0

Zur öffentlichen Veröffentlichung 2011 6. Juli 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zur PSIRT-Sicherheitsempfehlung für *Denial-of-Service-Schwachstellen beim Cisco Content Services Gateway* und bietet Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten einsetzen können.

Merkmale der Schwachstelle

Das Cisco Content Services Gateway - Second Generation (CSG2) weist eine Schwachstelle bei der Verarbeitung einer Reihe speziell erstellter ICMP-Pakete auf. Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriffe per Remote-Zugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann das betroffene Gerät neu geladen werden, was zu einer Diensteverweigerung (Denial of Service, DoS) führt. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung wird durch eine Reihe von ICMP-Paketen generiert.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-2064 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-20110706-csg.

Überblick über die Risikominderungstechnik

Cisco Geräte bieten verschiedene Gegenmaßnahmen für diese Schwachstelle. 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 von Transit-Zugriffskontrolllisten (tACLs) effektive Möglichkeiten zur Verhinderung von Exploits.

Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstelle auszunutzen.

Die Cisco Adaptive Security Appliance der Serie ASA 5500 und das Firewall Services Module (FWSM) für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 bieten zudem effektiven Schutz vor Exploits, indem sie Transit Access Control Lists (tACLs) verwenden.

Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstelle auszunutzen.

Die effektive Nutzung von Cisco Intrusion Prevention System (IPS)-Ereignisaktionen bietet Transparenz und Schutz vor Angriffen, die diese Schwachstelle 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 Schwachstelle 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 dieser Schwachstelle bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte ICMP-Pakettypen, einschließlich Echoanfrage, Echo-Antwort, Host-unreachable, Traceroute, Paket zu groß, Zeit überschritten und nicht erreichbar, 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 protocol ! access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo-reply access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 host-unreachable access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 traceroute access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 unreachable ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 echo access-list 150 deny icmp
any 192.168.60.0 0.0.0.255 echo-reply access-list 150 deny icmp any 192.168.60.0
0.0.0.255 host-unreachable access-list 150 deny icmp any 192.168.60.0 0.0.0.255
traceroute access-list 150 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded access-list 150
```

```
deny icmp any 192.168.60.0 0.0.0.255 unreachable ! !-- 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.

Identifizierung:Transit-Zugriffskontrolllisten

Nachdem der Administrator die tACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der gefilterten ICMP-Pakettypen, einschließlich Echo-Anforderung, Echo-Antwort, Host-unreachable, Traceroute, Paket zu groß, Zeit überschritten und nicht erreichbar. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Beispielausgabe für **show ip access-lists 150**:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
    20 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
    30 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-unreachable
    40 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
    50 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big
    60 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded
    70 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable
    80 deny icmp any 192.168.60.0 0.0.0.255 echo (12 matches)
    90 deny icmp any 192.168.60.0 0.0.0.255 echo-reply (26 matches)
    100 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable (10 matches)
    110 deny icmp any 192.168.60.0 0.0.0.255 traceroute (7 matches)
    120 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big (9 matches)
    130 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded (2 matches)
    140 deny icmp any 192.168.60.0 0.0.0.255 unreachable (18 matches)
    150 deny ip any any
router#
```

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

- **12 ICMP-Echoanforderungspakete** für ACE-Leitung 80
- **26 ICMP-Echoantwortpakete** für ACE-Leitung 90
- **10 nicht erreichbare ICMP-Host**-Pakete für ACE-Leitung 100
- **7 ICMP-Traceroute**-Pakete für ACE-Leitung 110
- **9 ICMP-Pakete zu groß** für ACE-Leitung 120
- **2 ICMP-**Pakete **mit Zeitüberschreitung** für ACE-Leitung 130
- **18 nicht erreichbare ICMP**-Pakete für ACE-Leitung 140

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.

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 möglicherweise versucht wird, die Schwachstelle auszunutzen. Den Administratoren wird empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, die Schwachstelle auszunutzen, oder ob es sich um legitime Datenflüsse handelt.

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

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

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
```

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

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  01 0984 0800     9
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  01 0911 0000     4
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   01 0B3E 0301     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   01 0B89 0030     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  01 0BD7 0200     7
Gi0/0         192.168.15.130  Gi0/1         192.168.60.239  01 0BD7 1100     3
Gi0/0         192.168.23.220  Gi0/1         192.168.60.239  01 0BD7 0300    11
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für die folgenden **ICMP-**Pakettypen: **ICMP-Echoanfrage (Hexadezimalwert 0800), Echo-Antwort (Hexadezimalwert 0000), Host-unerreichbar (Hexadezimalwert 0301), Traceroute (Hexadezimalwert 0030), Packet-to-Big (Packet-To-Big (Packet-To-Big) Hexadezimalwert 0200), Zeitüberschreitung (Hexadezimalwert 1100) und nicht erreichbar (Hexadezimalwert 0300)**.

Um nur die Datenverkehrsflüsse für die zuvor genannten ICMP-Pakettypen anzuzeigen, muss der Befehl **show ip cache flow | include SrcIf| _01_.*(0800|0000|0301|0030|0200|1100|0300)_** zeigt die zugehörigen ICMP NetFlow-Datensätze wie folgt an:

ICMP-Datenflüsse

```
router#show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|0200|1100|0300)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  01 0984 0800     9
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  01 0911 0000     4
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   01 0B3E 0301     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   01 0B89 0030     1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  01 0BD7 0200     7
Gi0/0         192.168.15.130  Gi0/1         192.168.60.239  01 0BD7 1100     3
Gi0/0         192.168.23.220  Gi0/1         192.168.60.239  01 0BD7 0300    11
```

```
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 dieser Schwachstelle bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte ICMP-Pakettypen, einschließlich Echoanfrage, Echo-Antwort, Host-unreachable, Traceroute, Paket zu groß, Zeit überschritten und nicht erreichbar, 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 protocol ! access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 echo access-list tACL-Policy extended permit
icmp host 192.168.100.1 192.168.60.0 255.255.255.0 echo-reply access-list tACL-Policy
extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 traceroute access-
list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 2
access-list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0
255.255.255.0 time-exceeded access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 unreachable ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
echo access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 echo-
reply access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
traceroute access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
2 access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 time-
exceeded access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
unreachable ! !-- 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
```

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der gefilterten ICMP-Pakettypen einschließlich Echo-Anforderung, Echo-Antwort, Host-unreachable, Traceroute, Paket zu groß, Zeit überschritten und

nicht erreichbar identifizieren. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Beispielausgabe für **show access-list tACL-Policy**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 13 elements
access-list tACL-Policy line 1 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 echo
access-list tACL-Policy line 2 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 echo-reply
access-list tACL-Policy line 3 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 traceroute
access-list tACL-Policy line 4 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 2
access-list tACL-Policy line 5 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 time-exceeded
access-list tACL-Policy line 6 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 unreachable
access-list tACL-Policy line 7 extended deny icmp any
     192.168.60.0 255.255.255.0 echo (hitcnt=9)
access-list tACL-Policy line 8 extended deny icmp any
     192.168.60.0 255.255.255.0 echo-reply (hitcnt=12)
access-list tACL-Policy line 9 extended deny icmp any
     192.168.60.0 255.255.255.0 traceroute (hitcnt=7)
access-list tACL-Policy line 10 extended deny icmp any
     192.168.60.0 255.255.255.0 2 (hitcnt=11)
access-list tACL-Policy line 11 extended deny icmp any
     192.168.60.0 255.255.255.0 time-exceeded (hitcnt=5)
access-list tACL-Policy line 12 extended deny icmp any
     192.168.60.0 255.255.255.0 unreachable (hitcnt=8)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=17)
fireall#
```

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

- **9 ICMP-Echo**-Pakete für ACE-Leitung 7
- **12 ICMP-Echoantwortpakete** für ACE-Leitung 8
- **7 ICMP-Traceroute**-Pakete für ACE-Leitung 9
- **11 "ICMP Packet-to-big"**-Pakete für ACE-Leitung 10
- **5 ICMP-**Pakete **mit Zeitüberschreitung** für ACE-Leitung 11
- **8 nicht erreichbare ICMP**-Pakete für ACE-Leitung 12

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 beschriebene Schwachstelle 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
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/2048 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.2.0.200/2945
         dst inside:192.168.60.33/0 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/48 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/512 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/4352  by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/768 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-*tACL-Richtlinie* protokollierten Nachrichten die **ICMP-**Pakettypen **echo request, echo-reply, traceroute, packet-too-big, time-beyond und unreachable 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.

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 beschriebene Schwachstelle auszunutzen. Beginnend mit dem Signatur-Update S580 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, kann die Schwachstelle mit der Signatur 38247/0 erkannt werden (Signature Name: Cisco Content Services Gateway Denial of Service). Signatur 38247/0 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.

Signatur 38247/0 wird ausgelöst, wenn mehrere über ICMP gesendete Pakete erkannt werden. Wenn diese Signatur ausgelöst wird, kann dies auf einen potenziellen Angriff auf die 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 beschriebene Schwachstelle 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 beschriebene Schwachstelle 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 der in diesem Dokument beschriebenen Schwachstelle zusammenhängen. Hierzu wird die IPS-Signatur 38247/0 (Signature Name: Cisco Content Services Gateway Denial of Service) verwendet. Nach dem Download des dynamischen Signatur-Updates für S580 wird mit dem Schlüsselwort **NR-38247/0** für die IPS-Signatur 38247/0 und dem Abfragetyp **Alle übereinstimmenden Ereignisse** auf der Cisco Security MARS-Appliance ein Bericht bereitgestellt, in dem die durch die IPS-Signatur erstellten Vorfälle aufgelistet werden.

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 1.0	6. Juli 2011	Erste öffentliche Veröffentlichung

Cisco Sicherheitsverfahren

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

Zugehörige Informationen

- Cisco Applied Mitigation Bulletins
- Cisco Security
- Cisco Security IntelliShield Alert Manager Service
- Cisco Leitfaden zum Absichern von Cisco IOS-Geräten
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- NetFlow-Leistungsanalyse
- Cisco Network Foundation Protection - Whitepaper
- Cisco Network Foundation Protection - Präsentationen
- Ein sicherheitsorientierter Ansatz für die IP-Adressierung
- Grundlegendes zum Schutz der Kontrollebene
- Sichern der Tool Command Language auf Cisco IOS
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- 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.