Identifizieren und Beheben von Schwachstellen im Cisco ACE Application Control Engine Module und der Cisco ACE 4710 Application Control Engine

Beratungs-ID: cisco-amb-20100811-ace

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100811-ace

Revision 1.1

Zum öffentlichen Release 2010, 11. August, 16:00 Uhr UTC (GMT)

Inhalt

Antwort von Cisco
Gerätespezifische Eindämmung und Identifizierung
Zusätzliche Informationen
Revisionsverlauf
Cisco Sicherheitsverfahren
Zugehörige Informationen

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zum PSIRT Security Advisory *Multiple Vulnerabilities im Cisco ACE Application Control Engine Module und der Cisco ACE 4710 Application Control Engine* und stellt Techniken zur Identifizierung und Eindämmung von Sicherheitsrisiken bereit, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

Schwachstellenmerkmale

Das Cisco ACE Application Control Engine-Modul und die Cisco ACE 4710 Application Control Engine bieten mehrere Schwachstellen. In diesen Unterabschnitten werden folgende Sicherheitslücken zusammengefasst:

Real-Time Streaming Protocol (RTSP) Inspection Denial of Service-Schwachstelle: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzerinteraktion per Remote-Zugriff ausgenutzt werden. Die erfolgreiche Ausnutzung dieser Schwachstelle kann zum Absturz des betroffenen Geräts führen, was zu einer Denial of Service (DoS)-Bedingung führt. Wiederholte Versuche, diese Schwachstelle auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor für die Ausnutzung besteht aus RTSP-Paketen mit TCP-Port 554.

Diese Schwachstelle wurde der CVE-Kennung CVE-2010-2822 zugewiesen.

HTTP, RTSP und Session Initiation Protocol (SIP) Inspection Denial of Service-Schwachstelle:

Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzerinteraktion per Remote-Zugriff ausgenutzt werden. Die erfolgreiche Ausnutzung dieser Schwachstelle kann zum Absturz des betroffenen Geräts führen, was zu einem DoS-Zustand führt. Wiederholte Versuche, diese Schwachstelle auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen.

Angriffsvektoren für die Ausnutzung werden durch Pakete mit den folgenden Protokollen und Ports bereitgestellt:

- HTTP mit TCP-Port 80
- RTSP mit TCP-Port 554
- SIP mit TCP-Port 5060

Diese Schwachstelle wurde der CVE-Kennung CVE-2010-2823 zugewiesen.

SSL-Denial-of-Service-Schwachstelle: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzerinteraktion per Remote-Zugriff ausgenutzt werden. Die erfolgreiche Ausnutzung dieser Schwachstelle kann zum Absturz des betroffenen Geräts führen, was zu einem DoS-Zustand führt. Wiederholte Versuche, diese Schwachstelle auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor für die Ausnutzung besteht aus SSL-Paketen mit TCP-Port 443.

Diese Schwachstelle wurde der CVE-Kennung CVE-2010-2824 zugewiesen.

SIP Inspection Denial of Service-Schwachstelle: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzerinteraktion per Remote-Zugriff ausgenutzt werden. Die erfolgreiche Ausnutzung dieser Schwachstelle kann zum Absturz des betroffenen Geräts führen, was zu einem DoS-Zustand führt. Wiederholte Versuche, diese Schwachstelle auszunutzen, könnten zu einem anhaltenden DoS-Zustand führen.

Angriffsvektoren für die Ausnutzung werden durch Pakete mit den folgenden Protokollen und Ports bereitgestellt:

- SIP mit TCP-Port 5060
- SIP mit UDP-Port 5060

Ein Angreifer könnte diese Sicherheitslücken mithilfe gefälschter Pakete ausnutzen.

Diese Schwachstelle wurde der CVE-Kennung CVE-2010-2825 zugewiesen.

Informationen zu angreifbarer, nicht betroffener und fester Software finden Sie im PSIRT Security Advisory, das unter dem folgenden Link verfügbar ist:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100811-ace

Überblick über die Eindämmungstechnik

Cisco Geräte bieten mehrere Gegenmaßnahmen für diese Schwachstellen. Administratoren sollten diese Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und dem Datenverkehr, der das Netzwerk durchläuft, betrachten. Dieser Abschnitt des Dokuments bietet einen Überblick über diese Techniken.

Die Cisco IOS® Software bietet mithilfe von iACLs (Infrastructure Access Control Lists) effektive Möglichkeiten zur Exploit-Prevention. Dieser Schutzmechanismus filtert und verwirft Pakete, die versuchen, diese Schwachstellen 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 können mithilfe von Transit Access Control Lists (tACLs) ebenfalls einen effektiven Schutz vor Sicherheitslücken bieten. Dieser Schutzmechanismus filtert und verwirft Pakete, die versuchen, diese Schwachstellen auszunutzen.

Die effektive Nutzung von Cisco Intrusion Prevention System (IPS)-Ereignisaktionen bietet Transparenz und Schutz vor Angriffen, die versuchen, diese Schwachstellen auszunutzen.

Cisco IOS NetFlow-Datensätze bieten Transparenz für netzwerkbasierte Nutzungsversuche.

Die Cisco IOS Software, die Cisco ASA und FWSM-Firewalls bieten Transparenz durch Syslog-Meldungen und Zählerwerte, die in der Ausgabe von **show-**Befehlen angezeigt werden.

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance bietet außerdem Transparenz durch Incidents, Abfragen und Ereignisberichte.

Risikomanagement

Organisationen wird empfohlen, ihre standardmäßigen Prozesse zur Risikobewertung und Risikominimierung zu befolgen, um die potenziellen Auswirkungen dieser Schwachstellen zu ermitteln. Triage bezieht sich auf das Sortieren von Projekten und die Priorisierung von Bemühungen, die am ehesten erfolgreich sind. Cisco hat Dokumente bereitgestellt, die Unternehmen bei der Entwicklung einer risikobasierten Triage-Funktion für ihre Informationssicherheitsteams unterstützen. Ankündigungen zu Sicherheitslücken sowie Triage and Prototyping unterstützen Unternehmen bei der Entwicklung wiederholbarer Sicherheitsbewertungs- und -reaktionsprozesse.

Gerätespezifische Eindämmung und Identifizierung

Vorsicht: Die Effektivität von Eindämmungsverfahren hängt von bestimmten Kundensituationen ab, z. B. Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischen Zielen. Wie bei allen Konfigurationsänderungen sollten Sie die Auswirkungen dieser Konfiguration vor der Anwendung der Änderung bewerten.

Spezifische Informationen zur Eindämmung 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: Infrastruktur-Zugriffskontrolllisten

Um Infrastrukturgeräte zu schützen und das Risiko, die Auswirkungen und die Effektivität direkter Infrastrukturangriffe zu minimieren, sollten Administratoren iACLs bereitstellen, um die Richtliniendurchsetzung für den an Infrastrukturgeräte gesendeten Datenverkehr durchzuführen. Administratoren können eine iACL erstellen, indem sie explizit zulassen, dass nur autorisierter

Datenverkehr an Infrastrukturgeräte gesendet wird, der den bestehenden Sicherheitsrichtlinien und -konfigurationen entspricht. Um Infrastrukturgeräte optimal zu schützen, sollten die bereitgestellten iACLs auf allen Schnittstellen, für die eine IP-Adresse konfiguriert wurde, in Eingangsrichtung angewendet werden. Eine iACL-Problemumgehung bietet keinen vollständigen Schutz vor diesen Schwachstellen, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die iACL-Richtlinie verweigert nicht autorisierte SSL-Pakete am TCP-Port 443, 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, und der Host 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der erforderliche Datenverkehr für das Routing und den Administratorzugriff zugelassen wird, bevor der gesamte nicht autorisierte Datenverkehr abgelehnt wird. Der Adressbereich der Infrastruktur sollte sich nach Möglichkeit vom Adressbereich für die Benutzer- und Servicesegmente unterscheiden. Mithilfe dieser Adressierungsmethode können iACLs erstellt und bereitgestellt werden.

Weitere Informationen zu iACLs finden Sie unter Protecting Your Core: Zugriffskontrolllisten für den Infrastrukturschutz.

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable port ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 ! !-- The following vulnerability-specific access control entry !-- (ACE) can aid in identification of attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 443 ! !-- Explicit deny ACE for traffic sent to addresses configured within !-- the infrastructure address space ! deny ip any 192.168.60.0 0.0.0.255 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and configurations ! !-- Apply iACL to interfaces in the ingress direction ! interface GigabitEthernet0/0 ip access-group Infrastructure-ACL-Policy in
```

Beachten Sie, dass eine Filterung mit einer Schnittstellenzugriffsliste die Übertragung von nicht erreichbaren ICMP-Nachrichten an die Quelle des gefilterten Datenverkehrs auslöst. Das Generieren dieser Meldungen kann unerwünschte Auswirkungen haben, wenn die CPU-Auslastung auf dem Gerät erhöht wird. In der Cisco IOS-Software ist die standardmäßig alle 500 Millisekunden erreichbare ICMP-Generierung auf ein Paket beschränkt. Die Generierung nicht erreichbarer ICMP-Nachrichten kann mithilfe des Schnittstellenkonfigurationsbefehls **no ip unreachables** deaktiviert werden. Die ICMP-Ratenbegrenzung ohne Erreichbarkeit kann mithilfe des globalen Konfigurationsbefehls **ip icmp rate-limit unreachable** interval-*in-ms* von der Standardeinstellung geändert werden.

Identifikation: Infrastruktur-Zugriffskontrolllisten

Nachdem der Administrator die iACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der SSL-Pakete am TCP-Port 443, die auf Schnittstellen gefiltert wurden, auf die die iACL angewendet wird. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show ip access-lists infrastructure-ACL-Policy**:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    20 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (3713 matches)
```

```
    30 deny ip any 192.168.60.0 0.0.0.255
router#
```

Im vorherigen Beispiel hat die Zugriffsliste *Infrastructure-ACL-Policy* **3713 SSL-**Pakete auf dem **TCP-**Port **443 (HTTPS)** für den Eintrag in der Zugriffskontrollliste (ACE) Zeile 20 verworfen.

Weitere Informationen zur Ermittlung von Incidents mit ACE-Zählern und Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.

Administratoren können mithilfe von Cisco Embedded Event Manager eine Instrumentierung bereitstellen, wenn bestimmte Bedingungen erfüllt sind, z. B. ACE-Zähleraufrufe. Das Applied Intelligence Whitepaper Embedded Event Manager in einem Sicherheitskontext enthält zusätzliche Informationen zur Verwendung dieser Funktion.

Identifikation: Protokollierung von Zugriffslisten

Die Option **log** und **log-input** access control list (ACL) bewirkt, dass Pakete protokolliert werden, die bestimmten ACEs entsprechen. Die **Log-Input-**Option ermöglicht die Protokollierung der Eingangs-Schnittstelle zusätzlich zu den IP-Adressen und Ports der Paketquelle und des Ziels.

Vorsicht: Die Protokollierung von Zugriffskontrolllisten kann sehr CPU-intensiv sein und muss mit größter Vorsicht erfolgen. Faktoren, die die CPU-Auswirkungen der ACL-Protokollierung beeinflussen, sind Protokollgenerierung, Protokollübertragung und Prozessswitching, um Pakete weiterzuleiten, die protokollfähigen ACEs entsprechen.

Für die Cisco IOS-Software kann der Befehl **ip access-list logging interval-in-ms** die Auswirkungen des durch die ACL-Protokollierung induzierten Prozess-Switching begrenzen. Der Befehl **logging rate-limit** *rate-per-second* [mit *Ausnahme* des Befehls loglevel] begrenzt die Auswirkungen von Protokollgenerierung und -übertragung.

Die CPU-Auswirkungen der ACL-Protokollierung können in der Hardware der Cisco Catalyst Switches der Serie 6500 und der Cisco Router der Serie 7600 mithilfe der Supervisor Engine 720 oder der Supervisor Engine 32 mithilfe optimierter ACL-Protokollierung behoben werden.

Weitere Informationen zur Konfiguration und Verwendung der ACL-Protokollierung finden Sie im Whitepaper Understanding Access Control List Logging Applied Intelligence.

Cisco IOS NetFlow

Identifikation: Identifikation des Datenverkehrs mithilfe von NetFlow-Datensätzen

Administratoren können Cisco IOS NetFlow auf Cisco IOS-Routern und -Switches konfigurieren, um die Identifizierung von Datenverkehrsflüssen zu erleichtern, die möglicherweise versuchen, diese Schwachstellen auszunutzen. Administratoren werden empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich um Versuche handelt, diese Sicherheitslücken auszunutzen, oder ob es sich um legitime Datenverkehrsflüsse 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         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016 01BB     1
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
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  06 0BD7 01BB    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 **SSL** am **TCP-**Port **443 (Hexadezimalwert 01BB)**.

Um nur die Datenverkehrsflüsse für SSL-Pakete am TCP-Port 443 (Hex-Wert 01BB) anzuzeigen, wird der Befehl **show ip cache flow angezeigt. | Srclf|_06_.*01BB** zeigt die zugehörigen TCP-NetFlow-Datensätze wie hier gezeigt an:

```
router#show ip cache flow | include SrcIf|_06_.*01BB
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  06 0BD7 01BB    11
router#
```

Cisco ASA- und FWSM-Firewalls

Eindämmung: Transit Access Control Lists

Zum Schutz des Netzwerks vor Datenverkehr, der an Eingangspunkten in das Netzwerk eingeht, z. B. Internetverbindungspunkte, Verbindungspunkte für Partner und Lieferanten oder VPN-Verbindungspunkte, wird Administratoren empfohlen, Zugriffskontrolllisten (ACLs) zu implementieren, um die Richtliniendurchsetzung durchzuführen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr an den Eingangspunkten in das Netzwerk eintritt, oder dass autorisierter Datenverkehr das Netzwerk entsprechend der bestehenden Sicherheitsrichtlinien und -konfigurationen durchquert. Eine tACL-Problemumgehung kann keinen vollständigen Schutz gegen diese Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte SSL-Pakete am TCP-Port 443, 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, und der Host 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der erforderliche Datenverkehr für das Routing und den Administratorzugriff zugelassen wird, bevor der gesamte nicht autorisierte Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie in den Transit Access Control Lists: Filtern am Netzwerk-Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable port ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 443 ! !-- The following vulnerability-specific access control entry !-- (ACE)
can aid in identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 443 ! !-- 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
```

Identifikation: Transit Access Control Lists

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der SSL-Pakete am TCP-Port 443 ermitteln, die gefiltert wurden. Administratoren werden empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich um Versuche handelt, diese Sicherheitslücken auszunutzen. Beispielausgabe für **show access-list tACL-Policy**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq https (hitcnt=3713)
access-list tACL-Policy line 2 extended deny tcp any
     192.168.60.0 255.255.255.0 eq https (hitcnt=221)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

Im obigen Beispiel hat die Zugriffsliste *tACL-Policy* **221 SSL-**Pakete auf dem **TCP-**Port **443 (HTTPS)**, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden, verworfen. Darüber hinaus kann die Syslog-Meldung *106023* wertvolle Informationen bereitstellen, darunter die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Portnummern sowie das IP-Protokoll für das abgelehnte Paket.

Identifikation: Firewall-Zugriffsliste Syslog-Meldungen

Die Firewall-Syslog-Meldung *106023* wird für Pakete generiert, die von einem Zugriffskontrolleintrag (ACE) abgelehnt werden, der das **log-**Schlüsselwort nicht enthält. Weitere Informationen zu dieser Syslog-Meldung finden Sie in der Systemprotokollmeldung zur Cisco Serie ASA 5500, 8.2 - 106023.

Informationen zum Konfigurieren von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 finden Sie unter Überwachung - Konfiguration der Protokollierung. Informationen zum Konfigurieren von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie in Monitoring the Firewall Services Module.

Im folgenden Beispiel **zeigt** die **Protokollierung Der Befehl | grep** *regex* extrahiert Syslog-Meldungen aus dem Protokollierungspuffer in der Firewall. Diese Nachrichten enthalten zusätzliche Informationen zu abgelehnten Paketen, die auf mögliche Versuche hinweisen könnten, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Sie können mit dem **grep**-Schlüsselwort verschiedene reguläre Ausdrücke verwenden, um nach bestimmten Daten in den protokollierten Nachrichten zu suchen.

Weitere Informationen zur Syntax regulärer Ausdrücke finden Sie unter Erstellen eines regulären Ausdrucks.

```
firewall#show logging | grep 106023
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/443 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL *tACL-Policy* protokollierten Meldungen **SSL-**Pakete für den **TCP**-Port **443 (HTTPS)** an den Adressblock, der betroffenen Geräten zugewiesen ist.

Weitere Informationen zu Syslog-Meldungen für ASA Security Appliances finden Sie in Systemprotokollmeldungen der Cisco Serie ASA 5500, 8.2. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie in den Protokollnachrichten für das Catalyst Switch der Serie 6500 und die Firewall Services Module der Cisco Serie 7600.

Weitere Informationen zur Untersuchung von Incidents mit 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 IPS-Appliances und -Servicemodule verwenden, um Bedrohungen

zu erkennen und Versuche zu verhindern, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Diese Sicherheitslücken können von den folgenden Signaturen erkannt werden:

- 27359/0 - RTSP-Sicherheitslücke
- 27599/0 - Cisco ACE SIP Inspection DoS

27359/0 - Real-Time Streaming Protocol Inspection-Schwachstelle

Ab dem Signaturupdate S507 für Sensoren mit Cisco IPS 6.x und höher kann diese Schwachstelle durch Signatur 27359/0 erkannt werden (Signaturname: Analysemethode für Echtzeit-Streaming-Protokolle). Die Signatur 27359/0 ist standardmäßig aktiviert, löst ein Ereignis mit *hohem* Schweregrad aus, weist eine Signaturtreue (SFR) von 90 auf und ist mit einer Standardereignisaktion **"reproduzieralert"** konfiguriert.

Die Signatur 27359/0 wird ausgelöst, wenn ein bestimmter Versuch zur Ausnutzung der durch den Cisco Identifikator CSCta85227 dokumentierten Schwachstelle erkannt wird. Das Erstellen dieser Signatur kann auf eine potenzielle Ausnutzung dieser Schwachstelle hinweisen.

27599/0 - Cisco ACE SIP Inspection DoS

Ab dem Signaturupdate S507 für Sensoren mit Cisco IPS 6.x und höher kann diese Schwachstelle durch Signatur 27599/0 erkannt werden (Signaturname: Cisco ACE SIP Inspection DoS). Die Signatur 27599/0 ist standardmäßig aktiviert, löst ein *mittelschweres* Ereignis aus, weist eine Signaturtreue-Bewertung (SFR) von 85 auf und ist mit einer Standardereignisaktion **von " produzieralarm"** konfiguriert.

Die Signatur 27599/0 wird ausgelöst, wenn ein bestimmter Versuch zur Ausnutzung der von den Cisco Identifikatoren CSCta65603 und CSCta71569 dokumentierten Schwachstellen erkannt wird. Das Erstellen dieser Signatur kann auf eine potenzielle Ausnutzung dieser Schwachstelle hinweisen.

Administratoren können Cisco IPS-Sensoren so konfigurieren, dass bei Erkennung eines Angriffs eine Ereignisaktion ausgeführt wird. Die konfigurierte Ereignisaktion führt vorbeugende oder abschreckende Kontrollen durch, um einen Angriff abzuwehren, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen.

Exploits, die gefälschte IP-Adressen verwenden, können dazu führen, dass eine konfigurierte Ereignisaktion den Datenverkehr von vertrauenswürdigen Quellen versehentlich blockiert.

Cisco IPS-Sensoren sind am effektivsten, wenn sie im Inline-Schutzmodus in Verbindung mit der Verwendung einer Ereignisaktion bereitgestellt werden. Der automatische Schutz vor Bedrohungen für Cisco IPS 6.x und Sensoren, die im Inline-Schutzmodus bereitgestellt werden, bietet Schutz vor Bedrohungen durch einen Angriff, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Der Schutz vor Bedrohungen wird durch eine Standardüberschrift erreicht, die eine Ereignisaktion für ausgelöste Signaturen mit einem *RiskRatingValue* über 90 ausführt.

Weitere Informationen zur Risikoeinstufung und zur Berechnung der Bedrohungsbewertung finden Sie unter Referenzrisikobewertung und Bedrohungsbewertung: Vereinfachtes IPS-Richtlinienmanagement.

Cisco Security Monitoring, Analysis and Response System

Identifikation: Cisco Security Monitoring, Analysis and Response System-Vorfälle

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance kann mithilfe der IPS-Signaturen 27359/0 (Signaturname: Real-Time Streaming Protocol Inspection Vulnerability (Sicherheitslücke bei Streaming-Protokollüberprüfung) und 27599/0 (Signaturname: Cisco ACE SIP Inspection DoS). Nachdem das dynamische Signaturupdate S507 heruntergeladen wurde, verwenden Sie das Schlüsselwort **NR-27359/0** für die IPS-Signatur 27359/0 oder **NR-27599/0** für die IPS-Signatur 27599/0 und einen Abfragetyp "All Matching Event Raw" Auf der Cisco Security MARS-Appliance wird ein Bericht erstellt, in dem die durch die IPS-Signatur erstellten Incidents aufgeführt sind.

Ab den Versionen 4.3.1 und 5.3.1 der Cisco Security MARS-Appliances wurde die Unterstützung für die Funktion zum Aktualisieren dynamischer Signaturen für Cisco IPS hinzugefügt. Diese Funktion lädt neue Signaturen von Cisco.com oder von einem lokalen Webserver herunter, verarbeitet und kategorisiert die empfangenen Ereignisse, die mit diesen Signaturen übereinstimmen, und fügt sie in Überprüfungsregeln und Berichte ein. Diese Updates ermöglichen die Normalisierung von Ereignissen und die Zuordnung von Ereignisgruppen und ermöglichen es der MARS-Appliance, neue Signaturen von den IPS-Geräten zu analysieren.

Vorsicht: Wenn dynamische Signaturaktualisierungen nicht konfiguriert werden, werden Ereignisse, die diesen neuen Signaturen entsprechen, in Abfragen und Berichten als *unbekannter Ereignistyp* angezeigt. Da MARS diese Ereignisse nicht in die Prüfungsregeln einbezieht, können keine Vorfälle für potenzielle Bedrohungen oder Angriffe im Netzwerk erstellt werden.

Diese Funktion ist standardmäßig aktiviert, muss aber konfiguriert werden. Wenn diese nicht konfiguriert ist, wird diese 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 **Help > About (Hilfe > Info) auswählen** und den Wert für die *IPS-Signaturversion überprüfen*.

Zusätzliche Informationen zu dynamischen Signatur-Updates sowie Anleitungen zum Konfigurieren dynamischer Signatur-Updates sind für die Cisco Security MARS 4.3.1- und 5.3.1-Versionen verfügbar.

Zusätzliche Informationen

Revisionsverlauf

Revision	11. August	Verweise auf die IPS-Signatur

1.1	2010	28301/0 entfernt.
Revision 1.0	11. August 2010	Erste Veröffentlichung.

Cisco Sicherheitsverfahren

Umfassende Informationen zur Meldung von Sicherheitsschwachstellen in Cisco Produkten, zum Erhalten von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Website von Cisco unter http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. Dazu gehören auch Anweisungen für Presseanfragen zu Cisco Sicherheitsmitteilungen. Alle Cisco Sicherheitsempfehlungen finden Sie unter http://www.cisco.com/go/psirt.

Zugehörige Informationen

- Von Cisco angewendete Warnmeldungen
- Cisco Security Intelligence Operations
- Cisco Security IntelliShield Alert Manager-Service
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Whitepaper zu Cisco IOS NetFlow
- NetFlow-Leistungsanalyse
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Cisco Intrusion Prevention System
- Downloads von Cisco IPS-Signaturen
- Cisco IPS-Seite für die Signatursuche
- Cisco Security Monitoring, Analysis and Response System
- Häufige Schwachstellen und Risikopositionen (CVE)