Identifizieren und Vermindern der Ausnutzung der Standard-Anmeldedaten für das Root-Konto auf der Cisco Media Experience Engine 5600

Identifizieren und Vermindern der Ausnutzung der Standard-Anmeldedaten für das Root-Konto auf der Cisco Media Experience Engine 5600

Beratungs-ID: cisco-amb-20110601-mxe

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110601-mxe

Version 1.0

Zur öffentlichen Veröffentlichung 2011 1. Juni 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zu den PSIRT Security Advisory *Default Credentials für root Account auf der Cisco Media Experience Engine 5600* und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten einsetzen können.

Merkmale der Schwachstelle

Die Cisco Media Experience Engine (MXE) 5600 enthält ein *Root*-Administratorkonto, das standardmäßig mit einem Standardkennwort aktiviert ist. Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriffe per Remote-Zugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung beliebigen Codes oder die Offenlegung von Informationen ermöglichen, sodass ein Angreifer Informationen über das betroffene Gerät erhalten kann. Der Angriffsvektor zur Ausnutzung wird durch SSH-Pakete über TCP-Port 22 und Telnet-Pakete über TCP-Port 23 generiert. Hinweis: Telnet ist auf der Cisco

MXE 5600 standardmäßig deaktiviert, kann jedoch als Angriffsvektor verwendet werden, wenn es manuell auf den betroffenen Geräten aktiviert wird.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-1623 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-20110601-mxe.

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 Infrastruktur-Zugriffskontrolllisten (Infrastructure Access Control Lists, iACLs) 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.

Cisco IOS NetFlow-Datensätze bieten Transparenz für netzwerkbasierte Exploit-Versuche.

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

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 IOS-Router und -Switches

Eindämmung: Infrastruktur-Zugriffskontrolllisten

Um Infrastrukturgeräte zu schützen und das Risiko, die Auswirkungen und die Effektivität direkter Angriffe auf die Infrastruktur zu minimieren, sollten Administratoren Infrastruktur-Zugriffskontrolllisten (iACLs) implementieren, um die Durchsetzung von Richtlinien für den an Infrastrukturgeräte gesendeten Datenverkehr zu ermöglichen. Administratoren können eine iACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen an die Geräte der Infrastruktur gesendet wird. Um einen maximalen Schutz für Infrastrukturgeräte zu gewährleisten, sollten bereitgestellte iACLs in Eingangsrichtung auf alle Schnittstellen angewendet werden, für die eine IP-Adresse konfiguriert wurde. Eine iACL-Problemumgehung kann keinen vollständigen Schutz vor dieser Schwachstelle bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die iACL-Richtlinie verweigert nicht autorisierte SSH-Pakete auf TCP-Port 22 und Telnet-Pakete auf TCP-Port 23, 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. Wenn möglich, sollte sich der Infrastruktur-Adressraum vom Adressraum unterscheiden, der für Benutzer- und Service-Segmente verwendet wird. Mit dieser Adressierungsmethode können Sie iACLs erstellen und bereitstellen.

Weitere Informationen zu iACLs finden Sie unter Protecting Your Core: Infrastructure Protection Access Control Lists (Schützen Ihres Kerns: Zugriffskontrolllisten für Infrastrukturschutz).

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 22 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 23 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 22 deny tcp any 192.168.60.0 0.0.0.255 eq 23 ! !-- 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 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.

Identifikation: Infrastruktur-Zugriffskontrolllisten

Nachdem der Administrator die iACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der SSH-Pakete auf dem TCP-Port 22 und der Telnet-Pakete auf dem TCP-Port 23, die auf Schnittstellen gefiltert wurden, auf die die iACL angewendet wird. Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Beispielausgabe für **show ip access-lists**:

```
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 ssh
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet
    30 deny tcp any 192.168.60.0 0.0.0.255 eq ssh (23 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq telnet (17 matches)
    50 deny ip any 192.168.60.0 0.0.0.255
router#
```

Im vorherigen Beispiel hat access list Infrastructure-ACL-Policy 23 SSH-Pakete auf dem TCP-Port 22 für die Zugriffskontrolllisteneintragsleitung (ACE) 30 und 17 Telnet-Pakete auf dem **TCP-**Port **23** für die ACE-Leitung 40 verworfen.

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.

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 (2409 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .349 .650 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

```
IP Flow Switching Cache, 278544 bytes
  89 active, 4007 inactive, 318 added
  4544 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             38      0.0         9    40      0.0       0.0      15.2
TCP-other          108      0.0         6    40      0.0       0.0      15.5
UDP-TFTP            10      0.0         4    28      0.0       0.0      15.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
UDP-other           73      0.0         7    28      0.0       0.0      15.5
Total:             229      0.0         7    35      0.0       0.0      15.5

SrcIf         SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.74.110  Et0/1          192.168.13.20   06 C8A7 D4BE     5
Et0/0         192.168.23.20   Et0/1          192.168.226.172 11 2123 540A     1
Et0/0         192.168.53.205  Et0/1          192.168.60.88   11 DEB7 0045     5
Et0/0         192.168.0.115   Et0/1          192.168.60.214  06 F73A 0050    11
Et0/0         192.168.0.30    Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.211.52  Et0/1          192.168.113.252 11 17AA 8F11    17
Et0/0         192.168.34.222  Et0/1          192.168.58.190  11 9A8F 2AD3     5
Et0/0         192.168.198.3   Et0/1          192.168.60.104  11 4F4D 0045     1
Et0/0         192.168.240.90  Et0/1          192.168.88.197  06 3D88 0017    15
Et0/0         192.168.0.96    Et0/1          192.168.60.126  06 9621 0017     3
Et0/0         192.168.155.22  Et0/1          192.168.80.13   06 1298 EB6A    10
Et0/0         192.168.0.20    Et0/1          192.168.60.78   06 1541 0050     3
Et0/0         192.168.0.2     Et0/1          192.168.60.195  06 5419 01BB     5
Et0/0         192.168.223.127 Et0/1          192.168.121.153 06 0613 17E5     7
Et0/0         192.168.0.28    Et0/1          192.168.60.101  06 B5C6 0017     2
Et0/0         192.168.92.207  Et0/1          192.168.43.167  11 1FF5 2815    11
Et0/0         192.168.0.28    Et0/1          192.168.60.139  06 24E9 0050     6
Et0/0         192.168.122.182 Et0/1          192.168.68.21   11 71C2 80BB    11
Et0/0         192.168.18.228  Et0/1          192.168.203.86  11 0630 77B4    16
Et0/0         192.168.0.218   Et0/1          192.168.60.248  06 531B 01BB    15
Et0/0         192.168.26.81   Et0/1          192.168.213.193 06 76D9 11B0     3
Et0/0         192.168.225.144 Et0/1          192.168.28.79   11 FF8F 299D    32
Et0/0         192.168.166.100 Et0/1          192.168.60.217  11 0B47 0045    10
Et0/0         192.168.49.15   Et0/1          192.168.139.203 11 D880 6D41     4
Et0/0         192.168.0.120   Et0/1          192.168.60.41   06 D24F 0016     6
Et0/0         192.168.0.109   Et0/1          192.168.60.189  06 B0B0 0016    11
Et0/0         192.168.0.65    Et0/1          192.168.60.136  06 6110 01BB     2
Et0/0         192.168.0.51    Et0/1          192.168.60.43   06 4090 0050    17
Et0/0         192.168.160.238 Et0/1          192.168.38.104  06 F54E DEE1    14
router#
```

Im vorherigen Beispiel gibt es mehrere Flüsse für SSH auf TCP-Port 22 (Hexadezimalwert 0016) und **Telnet** auf **TCP-**Port **23 (Hexadezimalwert 0017)**.

Um nur die Datenverkehrsflüsse für SSH-Pakete auf TCP-Port 22 (Hexadezimalwert 0016) und Telnet-Pakete auf TCP-Port 23 (Hexadezimalwert 0017) anzuzeigen, muss der Befehl **ip cache flow anzeigen. | include SrcIf|**_06_.*0016|0017 zeigt die zugehörigen TCP NetFlow-Datensätze wie folgt an:

TCP-Flows

```
router#show ip cache flow | include SrcIf|_06_.*0016|0017
SrcIf         SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.0.30     Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.0.120    Et0/1          192.168.60.41   06 D24F 0017     6
Et0/0         192.168.0.109    Et0/1          192.168.60.189  06 B0B0 0016    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 SSH-Pakete auf dem TCP-Port 22 und Telnet-Pakete auf dem TCP-Port 23, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen Geräten verwendet wird. Der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

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

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 22 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 23 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq
22 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 23 !
!-- 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 SSH-Pakete auf TCP-Port 22 und Telnet-Pakete auf TCP-Port 23 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; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=485)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=29)
access-list tACL-Policy line 3 extended deny tcp any
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=58)
access-list tACL-Policy line 4 extended deny tcp any
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=16)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste tACL-Policy **58 SSH-**Pakete auf dem **TCP-Port 22** und **16 Telnet-**Pakete auf dem **TCP-Port 23** verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden. Darüber hinaus kann die Syslog-Meldung *106023* nützliche Informationen bereitstellen, z. B. die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Port-Nummern und 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 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
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.194/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.164/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.106/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.241/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.169/1025
 dst inside:192.168.60.56/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.36/1025
 dst inside:192.168.60.202/22 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-tACL-Richtlinie protokollierten Meldungen **SSH-**

Pakete für den **TCP-Port 22** und **Telnet**-Pakete für den **TCP-Port 23 an,** die an den den Infrastrukturgeräten zugewiesenen Adressblock gesendet wurden.

Weitere Informationen zu Syslog-Meldungen für ASA Security Appliances finden Sie in Cisco ASA 5500 Series System Log Messages, 8.2. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie in den Protokollnachrichten des Catalyst Switches der Serie 6500 und des Cisco Routers der Serie 7600, Protokollierungssystem für Firewall-Services-Module.

Weitere Informationen zur Untersuchung von Vorfällen mithilfe von Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.

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	1. Juni 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
- Erkennung von und Beseitigung von TTL-Ablaufangriffen
- Ein sicherheitsorientierter Ansatz für die IP-Adressierung
- Gegenmaßnahmen für die böswillige Verwendung von IPv6-Typ-0-Routing-Headern
- Sichern der Tool Command Language auf Cisco IOS

- Cisco Firewall-Produkte - Startseite auf Cisco.com
- 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.