Identifizierung und Beseitigung von Schwachstellen bei der Remote-Codeausführung der Cisco Unified Service Monitor-, Cisco Unified Operations Manager- und CiscoWorks LAN Management-Lösung

Identifizierung und Beseitigung von Schwachstellen bei der Remote-Codeausführung der Cisco Unified Service Monitor-, Cisco Unified Operations Manager- und CiscoWorks LAN Management-Lösung

Beratungs-ID: cisco-amb-20110914-cusm-lms

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110914-cusm-lms

Version 1.0

Zur öffentlichen Veröffentlichung 2011 14. September 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses "Applied Mitigation Bulletin" ist ein Begleitdokument zu den folgenden PSIRT-Sicherheitsempfehlungen und bietet Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können:

- *Schwachstellen in Cisco Unified Service Monitor und Cisco Unified Operations Manager bei der Remote-Codeausführung*

- *Schwachstellen der CiscoWorks LAN Management-Lösung bei der Codeausführung per Fernzugriff*

Merkmale der Schwachstelle

Die Cisco Unified Service Monitor-Software, die Cisco Unified Operations Manager-Software und die CiscoWorks LAN Management Solution (LMS)-Software weisen zwei Schwachstellen auf, die es einem nicht authentifizierten Angreifer aus der Ferne ermöglichen könnten, beliebigen Code auf den betroffenen Geräten auszuführen. Beide Schwachstellen können ohne Authentifizierung und ohne Eingreifen der Endbenutzer remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstellen kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor für die Ausnutzung besteht aus vorgefertigten Paketen, die den TCP-Port 9002 verwenden. Diesen Schwachstellen wurde CVE-2011-2738 zugewiesen.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie in den PSIRT-Sicherheitsempfehlungen unter den folgenden Links: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-cusm und https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-lms.

Überblick über die Risikominderungstechnik

Cisco Geräte bieten eine Reihe von Gegenmaßnahmen für diese Sicherheitslücken. Den Administratoren wird empfohlen, diese Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs im Netzwerk zu betrachten. Dieser Abschnitt des Dokuments bietet einen Überblick über diese Techniken.

Die Cisco IOS Software bietet mithilfe von Infrastruktur-Zugriffskontrolllisten (Infrastructure Access Control Lists, iACLs) effektive Möglichkeiten zur Verhinderung von Exploits.

Dieser Schutzmechanismus filtert und löscht 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 bieten zudem effektiven Schutz vor Exploits, indem sie Transit Access Control Lists (tACLs) verwenden.

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

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.

Risikomanagement

Unternehmen wird empfohlen, ihre standardmäßigen Risikobewertungs- und Minderungsprozesse zu befolgen, um die potenziellen Auswirkungen von [dieser Schwachstelle|diesen Schwachstellen] 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

Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und betrieblichen Aufgaben 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 diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die iACL-Richtlinie verweigert nicht autorisierte Pakete auf dem TCP-Port 9002, 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 port
```

```
!
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9002
 !
!-- 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 9002
 !
!-- 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 Pakete auf dem TCP-Port 9002, 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 Schwachstellen 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 9002
20 deny tcp any 192.168.60.0 0.0.0.255 eq 9002 (11 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#
```

Im vorherigen Beispiel hat *access list Infrastructure-ACL-Policy* **11** Pakete auf dem **TCP-**Port **9002** verworfen für access control list entry (ACE) line 20.

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, die diese Schwachstellen ausnutzen können. Den Administratoren wird empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen, oder ob es sich um legitime Datenflüsse handelt.

```
router#show ip cache flow
IP packet size distribution (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  06 0984 232A     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 232A     3
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 232A     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 232A     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  06 0BD7 232A     1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
Gi0/0         192.168.48.69   Gi0/1         192.168.62.49   11 CB42 8B61     7
Gi0/0         192.168.0.74    Gi0/1         192.168.60.81   06 D542 0050     3
Gi0/0         192.168.0.53    Gi0/1         192.168.60.223  06 34C7 01BB     4
Gi0/0         192.168.221.121 Gi0/1         192.168.175.14  06 187B 34AA    11
Gi0/0         192.168.0.50    Gi0/1         192.168.60.185  06 4445 0050     5
Gi0/0         192.168.247.75  Gi0/1         192.168.123.123 11 BBA5 76E1     5
Gi0/0         192.168.0.183   Gi0/1         192.168.60.66   06 D0A8 232A     1
Gi0/0         192.168.216.117 Gi0/1         192.168.83.71   06 D102 9D1C    10
Gi0/0         192.168.135.87  Gi0/1         192.168.60.226  11 BBF9 0045     4
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für den **TCP**-Port **9002 (Hexadezimalwert 232A)**.

Um nur die Datenverkehrsflüsse für Pakete auf dem TCP-Port 9002 (Hexadezimalwert 232A) anzuzeigen, wird der **IP-Cache-Fluss angezeigt. | include SrcIf|**_*06_.*232A* zeigt die zugehörigen TCP NetFlow-Datensätze wie folgt an:

TCP-Flows

```
router#show ip cache flow | include SrcIf|_06_.*232A
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 232A     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 232A     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 232A     5
Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 06 0B89 232A 1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  06 0BD7 232A     1
Gi0/0 192.168.0.183 Gi0/1 192.168.60.66 06 D0A8 232A 1
router#
```

Cisco ASA und FWSM-Firewalls

Eindämmung: Transit-Zugriffskontrolllisten

Um das Netzwerk vor Datenverkehr zu schützen, der am Eingangspunkt in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Verbindungspunkte für Partner und Lieferanten oder VPN-Verbindungspunkte, sollten Administratoren tACLs bereitstellen, um die Richtlinien durchzusetzen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter

Datenverkehr an den Eingangs-Access Points in das Netzwerk eindringt, oder indem sie autorisiertem Datenverkehr gestatten, das Netzwerk gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen zu passieren. Eine tACL-Problemumgehung kann keinen vollständigen Schutz vor diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte Pakete auf dem TCP-Port 9002, 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 port
! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 9002 !
!-- 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 9002 !
!-- 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 Pakete auf dem TCP-Port 9002 identifizieren. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für **show access-list tACL-Policy**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 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 9002 (hitcnt=34)
access-list tACL-Policy line 2 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 9002 (hitcnt=119)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste *tACL-Policy* **119** Pakete auf dem **TCP-Port 9002** verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden.

Identifizierung: Firewall Access List, Syslog-Meldungen

Die Firewall-Syslog-Meldung *106023* wird für Pakete generiert, die von einem Zugriffskontrolleintrag (Access Control Entry, ACE) abgelehnt wurden, für die kein **log-**

Schlüsselwort vorhanden ist. Weitere Informationen zu dieser Syslog-Meldung finden Sie in Cisco ASA 5500 Series System Log Message, 8.2 - 106023.

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

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

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

```
firewall#show logging | grep 106023
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/9002 by access-group "tACL-Policy"
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/9002 by access-group "tACL-Policy"
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/9002 by access-group "tACL-Policy"
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/9002 by access-group "tACL-Policy"
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/9002 by access-group "tACL-Policy"
  Sep 14 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/9002 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-*tACL-Richtlinie* protokollierten Nachrichten Pakete für den **TCP-Port 9002 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.

Zusätzliche Informationen

Revisionsverlauf

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 Leitfaden zum Absichern von Cisco IOS-Geräten
- Überblick über die XSS-Bedrohungsvektoren (Cross-Site Scripting)
- 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.