Identifizieren und Verringern der Ausnutzung der offenen Abfrageschnittstelle in Cisco Unified Communications Manager und Presence Server

Identifizieren und Verringern der Ausnutzung der offenen Abfrageschnittstelle in Cisco Unified Communications Manager und Presence Server

Beratungs-ID: cisco-amb-20110824-cucm-cups

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-cups

Version 1.0

Zur öffentlichen Veröffentlichung 2011 24. August 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zur *offenen Abfrageschnittstelle* PSIRT Security Advisory *in Cisco Unified Communications Manager und Presence Server* und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten einsetzen können.

Merkmale der Schwachstelle

Cisco Unified Communications Manager (CUCM) und Cisco Unified Presence Server (CUPS) weisen eine Schwachstelle im Open SQL-Abfrageinterface auf. Diese Schwachstelle kann per Fernzugriff ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, können Informationen offen gelegt werden, sodass ein Angreifer Informationen über das betroffene Gerät erhalten kann. Der Angriffsvektor für die Ausnutzung besteht aus HTTPS-Paketen mit TCP-Port 443 und TCP-Port 8443.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-1643 zugewiesen.

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.

Mit tACLs können Sie außerdem einen effektiven Schutz vor Exploits gewährleisten, indem Sie 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 einsetzen.

Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstelle 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: 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 HTTPS-Pakete auf TCP-Port 443 und TCP-Port 8443, 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 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 access-
list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 !
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
! access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp
any 192.168.60.0 0.0.0.255 eq 8443 !
!-- 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 HTTPS-Pakete auf TCP-Port 443 und TCP-Port 8443, die gefiltert wurden. 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 tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
    30 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (12 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (26 matches)
    50 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 HTTPS**-Pakete auf **TCP-Port 443** für ACE-Leitung 30
- **26 HTTPS**-Pakete auf **TCP-Port 8443** für ACE-Leitung 40

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 06 0984 01BB 8
Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 06 0911 20FB 2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   11 0B3E 00A1     4
Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 06 0B89 20FB 3
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     2
Gi0/0 192.168.12.185 Gi0/1 192.168.60.239 06 0BD7 01BB 8
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 HTTPS auf dem **TCP-**Port **443 (Hexadezimalwert 01BB)** und dem **TCP-**Port **8443 (Hexadezimalwert 20FB)**.

Um nur die Datenverkehrsflüsse für HTTPS-Pakete auf TCP-Port 443 (Hexadezimalwert 01BB) und TCP-Port 8443 (Hexadezimalwert 20FB) anzuzeigen, wird der **IP-Cache-Fluss angezeigt. |**

include SrcIf|_06_.*(01BB|20FB)_ zeigt die zugehörigen TCP NetFlow-Datensätze wie folgt an:

TCP-Flows

```
router#show ip cache flow | include SrcIf|_06_.*(01BB|20FB)_
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0 192.168.12.110 Gi0/1 192.168.60.163 06 092A 01BB 6
Gi0/0 192.168.11.230 Gi0/1 192.168.60.20 06 0C09 01BB 1
Gi0/0 192.168.11.131 Gi0/1 192.168.60.245 06 0B66 20FB 18
Gi0/0 192.168.13.7 Gi0/1 192.168.60.162 06 0914 01BB 1
Gi0/0 192.168.41.86 Gi0/1 192.168.60.27 06 0B7B 20FB 2
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 HTTPS-Pakete auf TCP-Port 443 und TCP-Port 8443, 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 443 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8443 !
!-- 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 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443 !
!-- 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 HTTPS-Pakete auf TCP-Port 443 und TCP-Port 8443 identifizieren, die gefiltert wurden. 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 https (hitcnt=5)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 8443 (hitcnt=42)
access-list tACL-Policy line 3 extended deny tcp any
     192.168.60.0 255.255.255.0 eq https (hitcnt=20)
access-list tACL-Policy line 4 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 8443 (hitcnt=17)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

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

- **20 HTTPS**-Pakete auf **TCP-Port 443** für ACE-Leitung 3
- **17 HTTPS**-Pakete auf **TCP-Port 8443** für ACE-Leitung 4

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
  Aug 24 2011 00:08:13: %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 24 2011 00:08:13: %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 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/8443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
```

```
        dst inside:192.168.60.115/8443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %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 24 2011 00:08:13: %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-Richtlinie* protokollierten Nachrichten **HTTPS-**Pakete für den **TCP-Port 443** und den **TCP-Port 8443 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

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	24. AUGUST 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 Intelligence Operations
- 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
- 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.