

Identifikation und Behebung der Directory-Traversal-Schwachstelle im Cisco Network Admission Control Manager

Identifikation und Behebung der Directory-Traversal-Schwachstelle im Cisco Network Admission Control Manager

Beratungs-ID: cisco-amb-20111005-nac

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20111005-nac>

Version 1.1

Zuletzt aktualisiert am 18. Oktober 2011 um 17:06 Uhr (GMT)

Zur öffentlichen Veröffentlichung 2011, 5. Oktober, 16:00 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 zur PSIRT Security Advisory *Directory Traversal Vulnerability in Cisco Network Admission Control Manager* und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

Merkmale der Schwachstelle

Der Cisco Network Admission Control Manager (Cisco NAC Manager) enthält eine Directory-Traversal-Schwachstelle. Diese Schwachstelle kann ohne Authentifizierung per Remote-Zugriff ausgenutzt werden und erfordert eine Endbenutzerinteraktion. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Offenlegung von Informationen ermöglichen, sodass ein Angreifer Informationen über das betroffene Gerät und/oder Netzwerk abrufen kann. Der Angriffsvektor für

die Ausnutzung besteht aus HTTPS-Paketen mit dem TCP-Port 443.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-3305 zugewiesen.

Überblick über Sicherheitslücken

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-20111005-nac>.

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, das Adaptive Security Appliance Services Module (ASASM) und das Firewall Services Module (FWSM) für Cisco Catalyst Switches der Serie 6500 sowie für Cisco Router der Serie 7600 bieten ebenfalls einen effektiven Exploit-Schutz mithilfe von Transit Access Control Lists (tACLs). 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, die Cisco ASA Appliances, ASASM- und FWSM-Firewalls bieten Transparenz durch Syslog-Meldungen und die 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

Vorsicht: Die Effektivität jeder 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, ASASM 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 HTTPS-Pakete auf dem 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. 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 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 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 unreachable** 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 HTTPS-Pakete auf dem TCP-Port 443, 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 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 (17 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#

```

Im vorherigen Beispiel hat *access list Infrastructure-ACL-Policy* **17** HTTPS-Pakete auf dem TCP-Port **443** für access control list entry (ACE) line 20 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.

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 aged 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(Idle(
-----	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

```

router#
SrcIf      SrcIPAddress  DstIf      DstIPAddress Pr SrcP DstP  Pkts
Gi0/0    192.168.10.201 Gi0/1    192.168.60.122 06 0984 01BB    9
Gi0/1     192.168.150.60 Gi0/0     10.89.16.226   11 0016 12CA   1
Gi0/0    192.168.13.97  Gi0/1    192.168.60.28  06 0B3E 01BB    5
Gi0/0    192.168.10.17 Gi0/1    192.168.60.77  06 0B89 01BB    4
Gi0/0     10.88.226.1    Gi0/1     192.168.202.22 11 007B 007B   1
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**).

Um nur die Datenverkehrsflüsse für **HTTPS**-Pakete auf dem **TCP-Port 443** (**Hexadezimalwert 01BB**) anzuzeigen, muss der Befehl **show ip cache flow | include SrcIf_06_.*01BB_** zeigt die zugehörigen **TCP NetFlow**-Datensätze wie folgt an:

```

router#show ip cache flow | include SrcIf|_06_.*01BB_
SrcIf      SrcIPAddress  DstIf      DstIPAddress Pr SrcP DstP  Pkts
Gi0/0    192.168.10.201 Gi0/1    192.168.60.122 06 0984 01BB    9
Gi0/0    192.168.13.97  Gi0/1    192.168.60.28  06 0B3E 01BB    5
Gi0/0    192.168.10.17 Gi0/1    192.168.60.77  06 0B89 01BB    4
router#

```

Cisco ASA, ASASM 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 dem **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. 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 443 !
!-- 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 !
!-- 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 dem TCP-Port 443 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; 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=34)
access-list tACL-Policy line 2 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=139)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#

```

Im vorherigen Beispiel hat die Zugriffsliste *tACL-Policy* **139 HTTPS-Pakete** auf dem **TCP-Port 443** 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 unter [Cisco Security Appliance System Log Message - 106023 \(Systemprotokollmeldung der Cisco Security Appliance - 106023\)](#).

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 oder die Cisco Security Appliance der Serie PIX 500 finden Sie unter [Monitoring the Security Appliance - Configuring and Managing Logs](#). 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
Oct 05 2011 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"
Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.205/2945
dst inside:192.168.60.33/443 by access-group "tACL-Policy"
Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.49/2946
dst inside:192.168.60.240/443 by access-group "tACL-Policy"
Oct 05 2011 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"
Oct 05 2011 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"
Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.155/2950
dst inside:192.168.60.250/443 by access-group "tACL-Policy"
```

firewall#

Im vorherigen Beispiel zeigen die für die *tACL-tACL-Richtlinie* protokollierten Meldungen **HTTPS**-Pakete für den **TCP-Port 443** an, die an den Adressblock gesendet wurden, der den betroffenen Geräten zugewiesen ist.

Weitere Informationen zu Syslog-Meldungen für ASA- und PIX-Sicherheits-Appliances finden Sie in den [Systemprotokoll-Meldungen der Cisco Security Appliance](#). 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	5. Oktober 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 Leitfaden zum Absichern von Cisco IOS-Geräten](#)
- [Cisco Sicherheitscenter](#)
- [Cisco IOS NetFlow - Startseite auf Cisco.com](#)
- [Cisco IOS NetFlow-Whitepaper](#)
- [NetFlow-Leistungsanalyse](#)
- [Cisco Network Foundation Protection - Whitepaper](#)
- [Cisco Network Foundation Protection - Präsentationen](#)
- [Cisco Firewall-Produkte - Startseite auf Cisco.com](#)
- [Cisco Security Monitoring, Analysis and Response System](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.