

Identifikation und Beseitigung von Sicherheitslücken in Data-Link Switching-Software von Cisco IOS

Identifikation und Beseitigung von Sicherheitslücken in Data-Link Switching-Software von Cisco IOS

Beratungs-ID: cisco-amb-20110928-dlsw

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-dlsw>

Version 1.0

Zur öffentlichen Veröffentlichung 2011 28. September 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 zum PSIRT Security Advisory für *Cisco IOS Software Data-Link Switching Vulnerability* und bietet Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können.

Merkmale der Schwachstelle

Die Cisco IOS Software enthält eine Schwachstelle bei der Verarbeitung von fehlerhaften DLS-Paketen (Data-Link Switching). Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriffe per Remote-Zugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Dienstverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung wird durch IP-Protokoll-91-Pakete generiert. Ein Angreifer könnte diese Verwundbarkeit mit gefälschten Paketen ausnutzen.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0945 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-20110928-dlsw>.

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 der folgenden Methoden einen effektiven Schutz vor Exploits:

- InfrastrukturZugriffskontrolllisten (iACLs)
- Unicast Reverse Path Forwarding (Unicast-RPF)
- IP Source Guard (IPSG)

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstelle auszunutzen, und überprüfen die Quell-IP-Adresse von.

Die ordnungsgemäße Bereitstellung und Konfiguration von Unicast RPF bietet einen effektiven Schutz vor Angriffen, bei denen Pakete mit gefälschten Quell-IP-Adressen verwendet werden. Unicast-RPF sollte so nahe wie möglich an allen Datenverkehrsquellen bereitgestellt werden.

Die ordnungsgemäße Bereitstellung und Konfiguration von IPSG bietet einen effektiven Schutz vor Spoofing-Angriffen auf der Zugriffsebene.

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 mit den folgenden Methoden einen effektiven Schutz vor Exploits:

- Transit-Zugriffskontrolllisten (tACLs)
- Unicast RPF

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstelle auszunutzen, und überprüfen die Quell-IP-Adresse von.

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

Die Firewalls Cisco IOS Software, Cisco ASA und Cisco FWSM bieten Transparenz durch Syslog-Meldungen und Leistungsindikatorwerte, die in der Ausgabe von **show**-Befehlen 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 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 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 DLSw-Pakete auf dem IP-Protokoll 91, 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 protocol
!
permit 91 host 192.168.100.1 192.168.60.0 0.0.0.255
!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
deny 91 any 192.168.60.0 0.0.0.255
!
!-- 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.

Eindämmung: Spoofing-Schutz

Unicast Reverse Path Forwarding

Die in diesem Dokument beschriebene Schwachstelle kann durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast Reverse Path Forwarding (Unicast RPF) als Schutzmechanismus gegen Spoofing bereitstellen und konfigurieren.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen vollständigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. Den Administratoren wird empfohlen, während der Bereitstellung dieser Funktion sicherzustellen, dass der entsprechende Unicast-RPF-Modus (flexibel oder strikt) konfiguriert wird, da legitimer Datenverkehr, der das Netzwerk durchquert, verworfen werden kann. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützten Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen finden Sie im [Funktionsleitfaden zur Unicast Reverse Path Forwarding Loose Mode](#).

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie im Whitepaper [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence.

IP-Quellschutz

IP Source Guard (IPSG) ist eine Sicherheitsfunktion, die den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen beschränkt, indem Pakete auf Basis der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierter IP-Source-Bindings gefiltert werden. Administratoren können IPSG verwenden, um Angriffe eines Angreifers zu verhindern, der versucht, Pakete durch Fälschung der Quell-IP-Adresse und/oder der MAC-Adresse zu fälschen. Bei ordnungsgemäßer Bereitstellung und Konfiguration bietet IPSG in Verbindung mit dem strikten Modus mit Unicast-RPF den effektivsten Spoofing-Schutz für die in diesem Dokument beschriebene Schwachstelle.

Weitere Informationen zur Bereitstellung und Konfiguration von IPSG finden Sie unter [Konfigurieren der DHCP-Funktionen und von IP Source Guard](#).

Identifikation: Infrastruktur-Zugriffskontrolllisten

Nachdem der Administrator die iACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der DLSw-Pakete auf dem IP-Protokoll 91, 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 91 host 192.168.100.1 192.168.60.0 0.0.0.255
20 deny 91 any 192.168.60.0 0.0.0.255 (8 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#
```

Im vorherigen Beispiel hat access list *Infrastructure-ACL-Policy* **8 DLSw-Pakete** verworfen **IP-Protokoll 91** für Zugriffskontrolllisten-Eingangsleitung 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.

Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Wenn Unicast RPF ordnungsgemäß in der gesamten Netzwerkinfrastruktur implementiert und konfiguriert ist, können Administratoren den *internen Steckplatz/Port des Schnittstellentyps* "show cef", die `show ip interface`, die `show cef drop`-Funktion, die Funktion "show ip cef switching statistics" und die `show ip traffic`-Befehle verwenden, um die Anzahl der von Unicast RPF blockierten Pakete zu identifizieren.

Hinweis: Ab Version 12.4(20)T der Cisco IOS-Software wurde der Befehl `show ip cef switching` durch die Funktion `show ip cef switching statistics` ersetzt.

Hinweis: Der Befehl `show | Regex starten` und `Befehl anzeigen | include regex`-Befehlsmodifizierer werden in den folgenden Beispielen verwendet, um die Ausgabe zu minimieren, die Administratoren analysieren müssen, um die gewünschten Informationen anzuzeigen. Weitere Informationen zu Befehlsmodifizierern finden Sie in den Abschnitten [show command](#) in der Cisco IOS Configuration Fundamentals Command Reference.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
ip verify: via=rx (allow default), acl=0, drop=7, sdrop=0
router#
```

Hinweis: `show cef interface type slot/port internal` ist ein ausgeblendeter Befehl, der vollständig in die Kommandozeile eingegeben werden muss. Die Befehlsvervollständigung steht dafür nicht zur Verfügung.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
IP verify source reachable-via RX, allow default, allow self-ping 7 verification
drops
 0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP           27           0           0           7         0       0
router#
```

```
router#show ip cef switching statistics feature
```

```
IPv4 CEF input features:
Path Feature Drop    Consume    Punt    Punt2Host  Gave route
RP PAS uRPF           7         0         0         0         0
```

Total 7 0 0 0 0 -- CLI Output Truncated -- router# router#**show ip traffic | include RPF**

7 no route, 7 unicast RPF, 0 forced drop

router#

Im vorhergehenden Abschnitt **show cef drop, show ip cef switching statistics feature** and **show ip traffic example**, Unicast RPF hat **7 global empfangene IP-Pakete** an allen Schnittstellen mit konfigurierter Unicast RPF verworfen, da die Quelladresse der IP-Pakete in der Forwarding Information Base von Cisco Express Forwarding nicht verifiziert werden konnte.

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	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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	5B	0000	0000	11

```

Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 5B 0000 0000 8
Gi0/1          192.168.150.60 Gi0/0          10.89.16.226      06 0016 12CA      1

Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 5B 0000 0000 2
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 Flows für DLSw auf IP-Protokoll 91 (Hexadezimalwert 5B).

Dieser Datenverkehr wird an Adressen innerhalb des Adressblocks 192.168.60.0/24 gesendet, der von den betroffenen Geräten verwendet wird. Die Pakete in diesen Flows können gefälscht sein und einen Versuch anzeigen, diese Schwachstelle auszunutzen. Den Administratoren wird empfohlen, diese Datenflüsse mit der Basisauslastung für DLSw-Datenverkehr zu vergleichen, der über das IP-Protokoll 91 gesendet wird. Außerdem sollten sie die Flüsse untersuchen, um zu ermitteln, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen.

Um nur die Datenverkehrsflüsse für DLSw-Pakete auf dem IP-Protokoll 91 (Hexadezimalwert 5B) anzuzeigen, wird der **IP-Cache-Fluss angezeigt**. | **include SrcIf|_5B_** zeigt die zugehörigen IP-Protokoll 91 NetFlow-Datensätze wie folgt an:

```

router#show ip cache flow | include SrcIf|_5B_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0 192.168.12.110 Gi0/1 192.168.60.163 5B 0000 0000 11
Gi0/0 192.168.11.230 Gi0/1 192.168.60.20 5B 0000 0000 13
Gi0/0 192.168.11.131 Gi0/1 192.168.60.245 5B 0000 0000 7
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 DLSw-Pakete auf dem IP-Protokoll 91, 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 protocol
! access-list tACL-Policy extended permit 91 host 192.168.100.1 192.168.60.0

```



```

255.255.255.0 !
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
! access-list tACL-Policy extended deny 91 any 192.168.60.0 255.255.255.0 !
!-- 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

```

Eindämmung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die in diesem Dokument beschriebene Schwachstelle kann durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast RPF als Spoofing-Schutzmechanismus bereitstellen und konfigurieren.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen vollständigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberroute zur Quell-IP-Adresse vorhanden ist. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützenden Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie in der Cisco Security Appliance Command Reference for [ip verify reverse path](#) und im Whitepaper [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence.

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der DLSw-Pakete auf dem IP-Protokoll 91 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 91 host 192.168.100.1
    192.168.60.0 255.255.255.0 (hitcnt=34)
access-list tACL-Policy line 2 extended deny 91 any
    192.168.60.0 255.255.255.0 (hitcnt=6)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#

```

Im vorherigen Beispiel hat die Zugriffsliste *tACL-Policy* **6 DLSw-Pakete** auf dem **IP-Protokoll 91** 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
```

```
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.18
dst inside:192.168.60.191 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.200
dst inside:192.168.60.33 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.99
dst inside:192.168.60.240 by access-group "tACL-Policy"
```

```
firewall#
```

Im vorherigen Beispiel zeigen die für die *tACL-tACL-Richtlinie* protokollierten Nachrichten potenziell gefälschte **DLSw**-Pakete für das **IP-Protokoll 91 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.

Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die Firewall-Syslog-Meldung *106021* wird für Pakete generiert, die von Unicast RPF abgelehnt wurden. Weitere Informationen zu dieser Syslog-Meldung finden Sie in [Cisco ASA 5500 Series System Log Message, 8.2 - 106021](#).

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 106021
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from
192.168.60.1 to 192.168.60.191 on interface outside
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from
192.168.60.1 to 192.168.60.33 on interface outside
```

Der Befehl **show asp drop** kann außerdem die Anzahl der Pakete identifizieren, die von der Unicast RPF-Funktion verworfen wurden, wie im folgenden Beispiel gezeigt:

```
firewall#show asp drop frame rpf-violated
Reverse-path verify failed                16
firewall#
```

Im vorherigen Beispiel hat Unicast RPF **16 Pakete** verworfen, die an Schnittstellen mit konfigurierter Unicast RPF empfangen wurden. Fehlende Ausgabe zeigt an, dass die Unicast-RPF-Funktion der Firewall keine Pakete verworfen hat.

Weitere Informationen zum Debuggen von Paketen oder Verbindungen, die über einen beschleunigten Sicherheitspfad verworfen wurden, finden Sie unter Cisco Security Appliance Command Reference (Cisco Security Appliance-Befehlsreferenz) für [show asp drop](#).

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	28. SEPTEMBER	Erste öffentliche
1.0	2011	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](#)
- [Verbesserungen der Unicast Reverse Path Forwarding für den Internet Service Provider](#)
- [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.