Identifikation und Beseitigung von Schwachstellen bei MPLS-Paketen in Cisco Catalyst Switches der Serien 6000, 6500 und 7600

Identifikation und Beseitigung von Schwachstellen bei MPLS-Paketen in Cisco Catalyst Switches der Serien 6000, 6500 und 7600

Beratungs-ID: cisco-amb-20070228-mpls

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070228-mpls

Version 1.0

Zur öffentlichen Veröffentlichung 2007 Februar 28 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Merkmale der Schwachstelle

Die Paketschwachstellen Cisco Catalyst der Serien 6000 und 6500 und Cisco Multiprotocol Label Switching (MPLS) der Serie 7600 können vom lokalen Segment ohne Authentifizierung und ohne Benutzerinteraktion ausgenutzt werden. Die Schwachstelle kann zu einem Denial of Service (DoS) führen. Der Angriffsvektor wird über einen MPLS-Frame (EtherType 0x8847 und 0x8848) generiert. Diese Schwachstelle ist nicht durch eine CVE-ID gekennzeichnet.

Dieses Dokument enthält Informationen, die Cisco Kunden bei der Identifizierung und Eindämmung von Angriffen auf MPLS-Paketschwachstellen in den Cisco Catalyst Serien 6000

und 6500 und den Cisco MPLS der Serie 7600 unterstützen.

Informationen über anfällige, nicht betroffene und feste Software finden Sie in der PSIRT-Sicherheitsempfehlung:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070228-mpls

Überblick über die Risikominderungstechnik

Cisco Geräte bieten verschiedene Gegenmaßnahmen für die MPLS-Paketschwachstellen der Cisco Catalyst Serien 6000 und 6500 und der Cisco Serie 7600. Dieses Dokument konzentriert sich auf die Risikominimierung für anfällige Cisco Catalyst-Systeme der Serien 6000 und 6500 und der Cisco Serie 7600, die sich im Kern- und Distribution-Layer hinter einem Switched Access Layer befinden. Die in diesem Dokument enthaltenen Eindämmungs- und Identifizierungstechniken müssen auf diesen Switches des Access-Layers verwendet werden, um Frames zu filtern, die zur Ausnutzung dieser Schwachstelle verwendet werden könnten.

Die präventivste Kontrolle, die Cisco Netzwerkgeräte bieten, ist die Verwendung von IOS VLAN Maps.

Beachten Sie, dass die Systeme der Cisco Catalyst Serien 6000 und 6500 sowie der Cisco Serie 7600 keine effektive Methode zur Filterung von MPLS-Frames bieten.

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

Spezifische Informationen über die Minderung und Identifizierung sind verfügbar für:

- Cisco IOS-Switches

Cisco IOS-Switches

Vorsicht: Die Effektivität der Risikominimierungstechnik 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.

Die folgende Liste von Switches der Catalyst IOS-Serie wurde als Screening-Geräte vor Systemen der Cisco Catalyst 6000- und 6500-Serie und der 7600-Serie getestet, um die MPLS-

Paketschwachstelle zu beheben:

- Switches der Cisco Catalyst 2960-Serie
- Switches der Cisco Catalyst 3550-Serie
- Switches der Cisco Catalyst 3750-Serie
- Switches der Cisco Catalyst 4500-Serie

Cisco Catalyst Switches der Serie 2960

Risikominderung: MAC-Zugriffsgruppen

MAC-Zugriffsgruppen können verwendet werden, um zu filtern, ob EtherType 0x8847- und EtherType 0x8848-Frames einen Port betreten. Damit die Eindämmung wirksam ist, muss die MAC-Zugriffsgruppe auf alle Ports in den gleichen Broadcast-Domänen wie das anfällige Gerät angewendet werden. Bei den Cisco Catalyst Switches der Serie 2960 kann nur die **MAC-Zugriffsgruppe** auf die Eingangsrichtung angewendet werden (**in** Schlüsselwörtern).

```
mac access-list extended ACL-Deny-MPLS

!-- Filter MPLS frames deny any any 0x8847 0x0 deny any any 0x8848 0x0 !-- Include other permit/deny MAC access list configuration commands !-- according to security policy, might or not end in "permit any any" permit any anyinterface FastEthernet0/10
switchport access vlan 200 mac access-group ACL-Deny-MPLS in
```

Identifizierung: MAC-Zugriffsgruppen

Der Befehl Cisco Catalyst 2960 Series **show access-lists hardware counters** privileged EXEC mode zeigt einen einzelnen globalen Zähler für Frames an, die von allen MAC-Zugriffslisten gelöscht wurden ("Drop: All frame count"), sowie einen einzelnen globalen Zähler für die Gesamtzahl der Bytes in diesen gelöschten Frames ("Drop: All bytes count").

```
Cat2960#show access-lists hardware counters
 L2 ACL INPUT Statistics
     Drop:                    All frame count: 165
     Drop:                    All bytes count: 19684
     Bridge Only:             All frame count: 7886666
     Bridge Only:             All bytes count: 551148321
     Forwarding To CPU:       All frame count: 682046
     Forwarding To CPU:       All bytes count: 266514745
.
.
.
```

Im Beispiel wurden 165 Frames von allen MAC-Zugriffsgruppen im Switch verworfen, mit einer Gesamtzahl von 19.684 Byte innerhalb dieser 165 verworfenen Frames.

Cisco Catalyst Switches der Serie 3550

Eindämmung: VLAN-Karten

VLAN-Zuordnungen für Catalyst-Switches der Serie 3550 können so konfiguriert werden, dass MPLS-Frames in einem VLAN gefiltert werden. Im folgenden Beispiel verfügen anfällige Geräte über Schnittstellen in den VLANs 162 und 200. Diese VLANs sind so konfiguriert, dass sie

eingehende MPLS-Frames auf dem Cisco Catalyst Switch der Serie 3550 verwerfen, der als Abschirmgerät dient:

```
mac access-list extended ACL-Match-MPLS

!-- Filter MPLS frames, !-- will apply "action drop" to frames permitted in this MAC access-list permit any any 0x8847 0x0 permit any any 0x8848 0x0 !-- Other permit/deny MAC access list configuration commands !-- according to security policy vlan access-map VMAP-Policy 10 action drop match mac address ACL-Match-MPLS vlan access-map VMAP-Policy 20 action forward vlan filter VMAP-Policy vlan-list 162,200
```

Risikominderung: MAC-Zugriffsgruppen

MAC-Zugriffsgruppen der Catalyst Serie 3550 können nach einem beliebigen EtherType-Wert filtern. Sie können verwendet werden, um Frames mit dem EtherType 0x8847 oder 0x8848 zu verweigern. Die Zugriffsgruppe muss auf alle Ports in der Broadcast-Domäne des anfälligen Geräts angewendet werden. Die Cisco Catalyst 3550 **MAC-Zugriffsgruppe** kann nur in die eingehende Richtung angewendet werden (**in** Schlüsselwort)

```
mac access-list extended ACL-Deny-MPLS
 deny   any any 0x8847 0x0
 deny   any any 0x8848 0x0

!-- Other permit/deny MAC access list configuration commands !-- according to the security policy, !-- might or might not end in "permit any any" permit any any
interface FastEthernet0/1 switchport access vlan 162 switchport mode access mac access-group ACL-Deny-MPLS in
```

Identifikation: MAC-Zugriffsgruppen und VLAN-Zuordnungen

Der Befehl Cisco Catalyst 3550 Series **show access-lists hardware counters** privileged EXEC mode zeigt einen einzelnen globalen Zähler für Frames an, die in MAC-Zugriffslisten oder VLAN-Zuordnungen verworfen wurden. Es gibt einen separaten Zähler für die Gesamtzahl der Bytes, die von beiden Funktionen verworfen wurden. Im folgenden Beispiel wurden 268 Frames verworfen, was einer Gesamtzahl von 21.177 Byte entsprach.

```
Cat3550#show access-lists hardware counters
Input Drops:              268 matches (21177 bytes)
Output Drops:             0 matches (0 bytes)
Input Forwarded:          183663467 matches (14669769830 bytes)
Output Forwarded:         0 matches (0 bytes)
Input Bridge Only:        0 matches (0 bytes)
Bridge and Route in CPU: 0 matches (0 bytes)
Route in CPU:             460962054 matches (29596575890 bytes)
```

Cisco Catalyst Switches der Serie 3750

Eindämmung: VLAN-Karten

VLAN-Zuordnungen für Catalyst-Switches der Serie 3750 können so konfiguriert werden, dass MPLS-Frames in einem VLAN gefiltert werden. Im folgenden Beispiel verfügt ein anfälliges Gerät über eine Schnittstelle in VLAN 163. Der Cisco 3750, der als Screening-Gerät dient, verwirft eingehende MPLS-Frames auf VLAN 163.

```
mac access-list extended ACL-Match-MPLS

!-- MPLS EtherTypes to drop permit any any 0x8847 0x0 permit any any 0x8848 0x0 !--
Include other permit/deny MAC access list configuration commands !-- according to
security policy. vlan access-map VMAP-Policy 10 action drop match mac address ACL-
Match-MPLS vlan access-map VMAP-Policy 20 action forward vlan filter VMAP-Policy
vlan-list 163
```

Risikominderung: MAC-Zugriffsgruppen

MAC-Zugriffsgruppen der Catalyst Serie 3750 können nach einem beliebigen EtherType-Wert filtern und verwendet werden, um Frames mit EtherType 0x8847 oder 0x8848 zu verweigern. Die Zugriffsgruppe muss auf alle Ports in der Broadcast-Domäne des anfälligen Geräts angewendet werden.

```
mac access-list extended ACL-Deny-MPLS
     deny   any any 0x8847 0x0
     deny   any any 0x8848 0x0

!-- Include other permit/deny MAC access list commands according to security policy
!-- might or might not end in "permit any any" permit any any interface
FastEthernet3/0/47 switchport access vlan 163 mac access-group ACL-Deny-MPLS in
```

Identifikation: MAC-Zugriffsgruppen und VLAN-Zuordnungen

Mit dem Befehl **show access-lists hardware counters** privileged EXEC mode (Zugriffslisten für Hardware-Zähler anzeigen) für die Cisco Catalyst Serie 3750 wird ein einzelner globaler Zähler für Frames angezeigt, die von allen MAC-Zugriffsgruppen oder VLAN-Zuordnungen verworfen wurden. Es gibt einen separaten globalen Zähler für die Gesamtzahl der Bytes, die von beiden Funktionen verworfen wurden.

```
Cat3750#show access-lists hardware counters
 L2 ACL INPUT Statistics
     Drop:                    All frame count: 18170
     Drop:                    All bytes count: 2999815
     Bridge Only:             All frame count: 614950
     Bridge Only:             All bytes count: 39483560
     Forwarding To CPU:       All frame count: 0
     Forwarding To CPU:       All bytes count: 0
.
.
.
```

In der vorherigen Ausgabe wurden 18.170 Frames von MAC-Zugriffsgruppen oder VLAN-Zuordnungen verworfen. Die Gesamtbyteanzahl in den verworfenen Frames betrug 2.999.815.

Cisco Catalyst Switches der Serie 4500

Die vorgeschlagene Reduzierung in der Cisco Catalyst Serie 4500 ist nur möglich, wenn die Sicherheitsrichtlinien nur IP-Frames zulassen. Die Implementierung des Befehls **mac access-list** ermöglicht das Filtern von nur einem vordefinierten Protokollsatz. Durch die vorgeschlagene Reduzierung der Anfälligkeit von Cisco Catalyst-MPLS-Paketen der Serien 6000 und 6500 sowie der Cisco 7600-Serie werden u. a. AppleTalk- und IPX-Frames verworfen.

Eindämmung: VLAN-Karten

VLAN-Maps für die Catalyst Serie 4500 bieten die Möglichkeit, anhand einer vordefinierten Liste von Protokolltypen zu filtern. Durch Filterung aller Nicht-IP-Frames kann die MPLS-Paketanfälligkeit der Cisco Catalyst Serien 6000 und 6500 sowie der Cisco Serie 7600 verringert werden. Im folgenden Beispiel verwirft VLAN 160 alle Nicht-IP-Frames, um ein anfälliges Gerät zu schützen, das über eine Schnittstelle in VLAN 160 verfügt.

```
mac access-list extended ACL-Match-Non-IP
 permit any any

!-- Indicates ALL NON-IP frames flowing thru the switch will be dropped vlan access-
map VMAP-Policy 10 action drop match mac address ACL-Match-Non-IP ! vlan filter VMAP-
Policy vlan-list 160
```

Reduzierung: Port-ACLs

Port-ACL (PACL) der Catalyst Serie 4500 kann die Anfälligkeit von Cisco Catalyst-MPLS-Paketen der Serien 6000 und 6500 sowie der Cisco Serie 7600 verringern. Die PACL in der Cisco Catalyst Serie 4500 kann in ein- oder ausgehender Richtung angewendet werden. Mit dem Konfigurationsbefehl für die **Access Group Mode-**Schnittstelle kann die Interaktion zwischen der PACL, der VLAN-Zuordnung und der Router-ACL gesteuert werden, die für den Port gelten.

```
mac access-list extended ACL-Deny-Non-IP
 deny   any any

!-- Drop all non-IP frames flowing through the switch ! interface GigabitEthernet2/48
switchport access vlan 160 switchport mode access mac access-group ACL-Deny-Non-IP
out access-group mode prefer port ! Default
```

Bitte beachten Sie, dass die VLAN-Zuordnungen und PACL-Funktionen der Cisco Catalyst Serie 4500 den Durchfluss von IP-Protokoll-Frames nicht blockieren (EtherTypes 0x0800 und 0x0806). Außerdem blockieren sie nicht die folgenden vom Switch selbst verarbeiteten oder generierten Frames:

- Spanning Tree 802.1d BPDU
- Cisco Shared Spanning Tree Protocol (SSTP)
- Cisco Discovery Protocol (CDP)
- Unidirectional Link Detection (UDLD)
- VLAN Trunking Protocol (VTP)

Identifikation: VLAN-Zuordnungen und PACL

Die Catalyst Serie 4500 implementiert Zähler pro MAC Access Control Entry (ACE). Bitte beachten Sie, dass die erforderliche Konfiguration zur Beseitigung der MPLS-Paketschwachstellen der Cisco Catalyst Serien 6000 und 6500 und der Cisco Serie 7600 Loopback-Frames blockieren würde (EtherType 0x9000). Das Verwerfen von Loopback-Frames externer Stationen durch die Catalyst Serie 4500 hat keine Auswirkungen auf den Betrieb. Da Loopback-Frames gelöscht werden, wird mit dem Befehl **show access-lists** des privilegierten EXEC-Modus die Anzahl der übereinstimmenden Frames fortlaufend erhöht. Die Standardeinstellung bei Cisco IOS-Geräten ist, alle 10 Sekunden einen Loopback-Frame zu senden (**Keepalive**-Schnittstellenkonfigurationsbefehl).

```
Cat4500#show access-lists
Extended MAC access list ACL-Deny-Non-IP
    deny   any any (1151 matches)
Extended MAC access list ACL-Match-Non-IP
    permit any any (820 matches)
```

In der Beispielausgabe wurden 1.151 Frames durch die in der Beispiel-PACL verwendete MAC-Zugriffskontrollliste und 820 Frames durch die VLAN-Map-Beispielkonfiguration verworfen.

Eindämmung: {Inhalt hier einfügen}

- Cisco Catalyst VLAN Access Lists (VACLs) der Serien 6000 und 6500 bieten *keine* effektive Lösung. VACLs verhindern nicht, dass MPLS-Frames den Routingprozessor erreichen, und filtern diese Frames auch nicht nach Upstream-Geräten.
- Die Implementierung der MAC Access Group-Funktion in der Cisco Catalyst Serie 2950 erlaubt keine Filterung von bezeichneten Paketen unabhängig von IP-Paketen und kann nicht als Screening-Gerät für die MPLS-Paketschwachstellen in den Cisco Catalyst Serien 6000 und 6500 und der Cisco Serie 7600 verwendet werden.

Zusätzliche Informationen

Revisionsverlauf

Version 1.0	28. Februar 2007	Erste Veröffentlichung.

Cisco Sicherheitsverfahren

Vollständige Informationen zur Meldung von Sicherheitslücken in Cisco Produkten, zum Erhalt von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dies beinhaltet Anweisungen für Presseanfragen bezüglich der Sicherheitshinweise von Cisco. Alle Cisco Sicherheitsankündigungen finden Sie unter http://www.cisco.com/go/psirt.

Zugehörige Informationen

- Cisco Applied Mitigation Bulletins
- Cisco Security
- Cisco 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
- Grundlegendes zum Schutz der Kontrollebene
- Sichern der Tool Command Language auf Cisco IOS
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Verhindern von ActiveX-Exploits mit Cisco Firewall Application Layer Protocol Inspection
- Verhindern von ActiveX-Exploits mit Cisco Application Control Engine Application Layer Protocol Inspection
- Cisco ACE Application Control Engine Module - Dokumentation
- Verbesserungen der Unicast Reverse Path Forwarding für den Internet Service Provider
- Cisco Intrusion Prevention System 6.x
- Cisco IPS 6.x - Signatur-Downloads
- Seite für die Suche nach Cisco IPS-Signaturen
- Cisco Security Monitoring, Analysis and Response System
- Cisco Security Agent
- 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.