Identificazione e mitigazione dello sfruttamento di Cisco Catalyst serie 6000, 6500 e 7600 MPLS Packet Vulnerability

Identificazione e mitigazione dello sfruttamento di Cisco Catalyst serie 6000, 6500 e 7600 MPLS Packet Vulnerability

ID advisory: cisco-amb-20070228-mpls

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

Revisione 1.0

Per la Pubblica Release 2007 Febbraio 28 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Caratteristiche di vulnerabilità

I pacchetti Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 Multiprotocol Label Switching (MPLS) sono vulnerabili e possono essere sfruttati dal segmento locale senza autenticazione e senza necessità di interazione da parte dell'utente. La vulnerabilità può causare una condizione DoS (Denial of Service). Il vettore di attacco viene rilevato tramite un frame MPLS (EtherType 0x8847 e 0x8848). Questa vulnerabilità non è indicata da un ID CVE.

Questo documento contiene informazioni per aiutare i clienti Cisco a identificare e mitigare i tentativi di sfruttare le vulnerabilità dei pacchetti Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 MPLS.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory:

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

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per la vulnerabilità dei pacchetti Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 MPLS. Questo documento si concentra sulla mitigazione per i sistemi Cisco Catalyst serie 6000 e 6500 vulnerabili e Cisco serie 7600 che si trovano nei livelli di core e distribuzione dietro un layer di accesso commutato. Le tecniche di mitigazione e identificazione contenute in questo documento devono essere usate su questi switch del livello di accesso per filtrare i frame che potrebbero essere usati per sfruttare questa vulnerabilità.

Il controllo più preventivo fornito dai dispositivi di rete Cisco è tramite l'uso delle mappe VLAN di IOS.

Notare che i sistemi Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 non sono efficaci nel filtraggio dei frame MPLS.

Gestione dei rischi

Si consiglia alle organizzazioni di seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di [questa vulnerabilità|queste vulnerabilità]. Triage si riferisce all'ordinamento dei progetti e all'assegnazione delle priorità agli sforzi che hanno maggiori probabilità di avere successo. Cisco ha fornito documenti che possono aiutare le organizzazioni a sviluppare una funzionalità di triage basata sui rischi per i team addetti alla sicurezza delle informazioni. Valutazione dei rischi per la vulnerabilità della sicurezza Gli annunci e la valutazione dei rischi e la creazione di prototipi possono aiutare le organizzazioni a sviluppare processi ripetibili di valutazione della sicurezza e di risposta.

Mitigazione e identificazione specifiche del dispositivo

Informazioni specifiche sulla mitigazione e l'identificazione sono disponibili per:

- Switch Cisco IOS

Switch Cisco IOS

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Il seguente elenco selezionato di switch Catalyst serie IOS è stato testato come dispositivi di screening davanti ai sistemi Cisco Catalyst serie 6000, 6500 e 7600 per ridurre la vulnerabilità dei pacchetti MPLS:

- Cisco Catalyst serie 2960
- Cisco Catalyst serie 3550
- Cisco Catalyst serie 3750
- Cisco Catalyst serie 4500

Switch Cisco Catalyst serie 2960

Attenuazione: gruppi di accesso MAC

I gruppi di accesso MAC possono essere usati per filtrare i frame EtherType 0x8847 e EtherType 0x8848 dall'accesso a una porta. Affinché la mitigazione sia efficace, il gruppo di accesso MAC deve essere applicato a tutte le porte negli stessi domini di trasmissione del dispositivo vulnerabile. Gli switch Cisco Catalyst serie 2960 permettono di applicare solo il **gruppo di accesso mac** alla direzione di input (**parola chiave in**)

```
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
```

Identificazione: gruppi di accesso MAC

Il comando Cisco Catalyst serie 2960 **show access-lists hardware counters** in modalità di esecuzione privilegiata visualizza un singolo contatore globale per i frame scartati da tutti gli elenchi di accesso MAC ("Drop: All frame count") e un singolo contatore globale per il numero totale di byte in tali frame scartati ("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
.
.
.
```

Nell'esempio, tutti i gruppi di accesso MAC hanno scartato 165 frame nello switch, per un totale di 19.684 byte all'interno dei 165 frame scartati.

Switch Cisco Catalyst serie 3550

Mitigazione: mappe VLAN

Le mappe VLAN del Catalyst serie 3550 possono essere configurate per filtrare i frame MPLS di una VLAN. Nell'esempio seguente, i dispositivi vulnerabili dispongono di interfacce nelle VLAN 162 e 200. Queste VLAN sono configurate per eliminare i frame MPLS in ingresso negli switch Cisco Catalyst serie 3550 che fungono da dispositivo di schermatura:

```
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
```

Attenuazione: gruppi di accesso MAC

I gruppi di accesso MAC Catalyst serie 3550 possono filtrare in base a un determinato valore EtherType. Possono essere utilizzati per bloccare i frame con EtherType 0x8847 o 0x8848. Il gruppo di accesso deve essere applicato a tutte le porte nel dominio di trasmissione del dispositivo vulnerabile. L'**access-group mac** Cisco Catalyst 3550 può essere applicato solo nella direzione in ingresso (**parola** chiave **in**)

```
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
```

Identificazione: gruppi di accesso MAC e mappe VLAN

Il comando Cisco Catalyst serie 3550 **show access-lists hardware counters** in modalità di esecuzione privilegiata visualizza un singolo contatore globale per i frame scartati dagli elenchi degli accessi MAC o dalle mappe VLAN. È disponibile un contatore separato per il numero totale di byte scartati da entrambe le funzionalità. Nell'esempio seguente, sono stati scartati 268 frame, per un totale di 21.177 byte.

```
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)
```

Switch Cisco Catalyst serie 3750

Mitigazione: mappe VLAN

Le mappe VLAN del Catalyst serie 3750 possono essere configurate per filtrare i frame MPLS di una VLAN. Nell'esempio seguente, un dispositivo vulnerabile ha un'interfaccia nella VLAN 163. Lo switch Cisco 3750 che funziona come dispositivo di screening scarta i frame MPLS in ingresso sulla 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
```

Attenuazione: gruppi di accesso MAC

I gruppi di accesso MAC Catalyst serie 3750 possono filtrare in base a un determinato valore EtherType e possono essere utilizzati per negare i frame con EtherType 0x8847 o 0x8848. Il gruppo di accesso deve essere applicato a tutte le porte nel dominio di trasmissione del dispositivo vulnerabile.

```
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
```

Identificazione: gruppi di accesso MAC e mappe VLAN

Il comando Cisco Catalyst serie 3750 **show access-lists hardware counters** in modalità di esecuzione privilegiata visualizza un singolo contatore globale per i frame scartati da tutti i gruppi di accesso MAC o dalle mappe VLAN. È disponibile un singolo contatore globale distinto per il numero totale di byte scartati da entrambe le funzionalità.

```
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
.
.
.
```

Nell'output precedente, 18.170 frame sono stati scartati da gruppi di accesso MAC o mappe VLAN. Il numero totale di byte nei frame scartati è stato di 2.999.815.

Switch Cisco Catalyst serie 4500

La riduzione proposta per Cisco Catalyst serie 4500 è possibile solo se la policy di sicurezza consente solo i frame IP. L'implementazione del comando **mac access-list** permette di filtrare solo un set predefinito di protocolli. La mitigazione proposta per i pacchetti Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 MPLS causerà, tra le altre cose, il rifiuto dei frame AppleTalk e IPX.

Mitigazione: mappe VLAN

Le mappe VLAN dei Catalyst serie 4500 consentono di filtrare i dati in base a un elenco predefinito di tipi di protocollo. Per ridurre la vulnerabilità dei pacchetti MPLS di Cisco Catalyst serie 6000 e 6500 e Cisco 7600, è possibile filtrare tutti i frame non IP. Nell'esempio seguente, la VLAN 160 scarta tutti i frame non IP per proteggere un dispositivo vulnerabile con un'interfaccia nella VLAN 160.

```
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
```

Mitigazione: ACL di porta

I pacchetti ACL (PACL) delle porte Catalyst serie 4500 possono ridurre la vulnerabilità dei pacchetti Cisco Catalyst serie 6000 e 6500 e dei pacchetti MPLS della serie 7600. Il PACL di Cisco Catalyst serie 4500 può essere applicato nella direzione in entrata o in uscita. Il comando di configurazione dell'interfaccia **access-group mode** può essere usato per controllare l'interazione tra il PACL, la mappa VLAN e l'ACL del router che si applica alla porta.

```
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
```

Le mappe VLAN e le funzionalità PACL di Cisco Catalyst serie 4500 non bloccheranno il flusso dei frame del protocollo IP (EtherType 0x0800 e 0x0806). Inoltre, non bloccheranno i seguenti frame elaborati o generati dallo switch stesso:

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

Identificazione: Mappe VLAN e PACL

Catalyst serie 4500 implementa contatori per MAC Access Control Entry (ACE). La configurazione richiesta per ridurre la vulnerabilità dei pacchetti Cisco Catalyst serie 6000 e 6500 e Cisco serie 7600 MPLS bloccherebbe i frame di loopback (EtherType 0x9000). Non è previsto alcun impatto operativo per Catalyst serie 4500 in modo da eliminare i frame di loopback delle stazioni esterne. A causa della perdita di frame di loopback, il comando **show access-lists** in modalità di esecuzione privilegiata incrementerà costantemente il numero di frame corrispondenti. Per impostazione predefinita, nei dispositivi Cisco IOS il frame di loopback viene inviato ogni 10 secondi (comando di configurazione dell'interfaccia **keepalive**).

```
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)
```

Nell'output dell'esempio, 1151 frame sono stati scartati dall'ACL MAC usato dal PACL di esempio, mentre 820 frame sono stati scartati dalla configurazione della mappa VLAN di esempio.

Attenuazione: {Inserire il contenuto qui}

- Gli elenchi degli accessi VLAN (VACL) dei Cisco Catalyst serie 6000 e 6500 *non*

forniscono una riduzione efficace dei rischi. I VACL non impediranno ai frame MPLS di raggiungere il processore di routing né filtreranno tali frame per i dispositivi upstream.
- L'implementazione di Cisco Catalyst serie 2950 della funzionalità MAC Access Group non consente di filtrare i pacchetti con etichetta indipendentemente dai pacchetti IP e non può essere utilizzata come dispositivo di screening per le serie Cisco Catalyst 6000 e 6500 e la vulnerabilità dei pacchetti MPLS Cisco serie 7600.

Ulteriori informazioni

Cronologia delle revisioni

Revisione 1.0	28 febbraio 2007	Pubblicazione iniziale.

Procedure di sicurezza di Cisco

Le informazioni complete sulla segnalazione delle vulnerabilità della sicurezza nei prodotti Cisco, su come ottenere assistenza in caso di incidenti relativi alla sicurezza e su come registrarsi per ricevere informazioni sulla sicurezza da Cisco, sono disponibili sul sito Web di Cisco all'indirizzo https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Ciò include istruzioni per le richieste della stampa relative agli avvisi di sicurezza Cisco. Tutti gli avvisi sulla sicurezza Cisco sono disponibili all'indirizzo http://www.cisco.com/go/psirt.

Informazioni correlate

- Bollettini sulla mitigazione applicata di Cisco
- Cisco Security
- Guida Cisco per fortificare i dispositivi Cisco IOS
- Informazioni sui vettori di minaccia XSS (Cross-Site Scripting)
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- Analisi delle prestazioni di NetFlow
- White paper su Cisco Network Foundation Protection
- Presentazioni di Cisco Network Foundation Protection
- Identificazione e mitigazione degli attacchi TTL in scadenza
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- Contromisure per l'utilizzo dannoso delle intestazioni di routing IPv6 di tipo 0
- Informazioni sulla protezione del Control Plane
- Protezione della lingua dei comandi degli strumenti su Cisco IOS
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Prevenzione degli attacchi ActiveX con Cisco Firewall Application Layer Protocol

Inspection
- Prevenzione degli attacchi ActiveX con Cisco Application Control Engine Application Layer Protocol Inspection
- Documentazione del modulo Cisco ACE Application Control Engine
- Miglioramenti unicast Reverse Path Forwarding per il provider di servizi Internet
- Cisco 6.x Intrusion Prevention System
- Download per le firme Cisco IPS 6.x
- Pagina di ricerca delle firme IPS Cisco
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco
- Cisco Security Agent
- Vulnerabilità ed esposizioni comuni (CVE)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).