Identificatie en beperking van benutting van Cisco Catalyst 6000, 6500 en Cisco 7600 Series MPLS-pakketkwetsbaarheid

Identificatie en beperking van benutting van Cisco Catalyst 6000, 6500 en Cisco 7600 Series MPLS-pakketkwetsbaarheid

Advies-ID: cisco-amb-20070228-mpls

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

Revisie 1.0

2007 Februari 28 16:00 UTC (GMT)

Inhoud

Cisco Response

Kwetsbaarheid Kenmerken

De pakketkwetsbaarheid van Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series Multiprotocol Label Switching (MPLS) kan zonder verificatie worden geëxploiteerd vanuit het lokale segment en er is geen gebruikersinteractie nodig. De kwetsbaarheid kan in een ontkenning van de dienst (Dos) voorwaarde resulteren. De aanvalsvector is via een MPLS frame (EtherType 0x847 en 0x848). Deze kwetsbaarheid wordt niet aangegeven door een CVE ID.

Dit document bevat informatie om Cisco-klanten te helpen bij het identificeren en verzachten van pogingen om de Cisco Catalyst 6000- en 6500-reeks en Cisco 7600 Series MPLS-pakketkwetsbaarheid te exploiteren.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory:

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

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor de Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series MPLS-pakketkwetsbaarheid. Dit document concentreert zich op beperking voor kwetsbare Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series systemen die zich in kern- en distributielagen achter een switched toegangslaag bevinden. De mitigatie- en identificatietechnieken in dit document moeten op deze switches van de toegangslaag worden gebruikt om frames te filteren die kunnen worden gebruikt om deze kwetsbaarheid te exploiteren.

De meest preventieve controle door Cisco-netwerkapparaten wordt geboden door het gebruik van IOS VLAN-kaarten.

Bericht dat de systemen van Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series niet effectief zijn in het filteren van MPLS-frames.

Risicobeheer

Organisaties wordt aangeraden om hun standaardprocessen voor risico-evaluatie en -beperking te volgen om de potentiële impact van [deze kwetsbaarheid|deze kwetsbaarheden] te bepalen. Triage verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk het meest succesvol zullen zijn. Cisco heeft documenten geleverd die organisaties kunnen helpen bij de ontwikkeling van een op risico gebaseerde triagecapaciteit voor hun informatieveiligheidsteams. Risico Triage voor Security Vulnerability aankondigingen en Risk Triage en Prototyping kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

Specifieke informatie over mitigatie en identificatie is beschikbaar voor:

- Cisco IOS-Switches

Cisco IOS-Switches

Waarschuwing: de effectiviteit van elke mitigatietechniek is afhankelijk van specifieke klantsituaties zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

De volgende geselecteerde lijst van Catalyst IOS-Series switches is getest als screeningapparaten voor Cisco Catalyst 6000- en 6500-Series- en 7600-Series-systemen om de MPLS-pakketkwetsbaarheid te verminderen:

- Cisco Catalyst 2960 Series
- Cisco Catalyst 3550 Series
- Cisco Catalyst 3750 Series
- Cisco Catalyst 4500 Series

Cisco Catalyst 2960 Series switches

Beperken: MAC-toegangsgroepen

MAC-toegangsgroepen kunnen worden gebruikt om EtherType 0x847- en EtherType 0x848-frames te filteren van het invoeren van een poort. Om de beperking effectief te maken, moet de MAC-toegangsgroep worden toegepast op alle poorten in dezelfde uitzenddomeinen als het kwetsbare apparaat. De switches van Cisco Catalyst 2960 Series staan alleen toe dat de **MAC-toegangsgroep** wordt toegepast op de invoerrichting (**in** trefwoord)

```
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
```

Identificatie: MAC-toegangsgroepen

De Cisco Catalyst 2960 Series **toont hardwaretellers met** een geprivilegieerde EXEC-modus en geeft één algemene teller weer voor frames die zijn gedropt door alle MAC-toegangslijsten ("Drop: All frame count") en één algemene teller voor het totale aantal bytes in die gedropte 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
.
.
.
```

In het voorbeeld werden 165 frames door alle MAC-toegangsgroepen in de switch laten vallen, met een totaal van 19.684 bytes binnen die 165 gedropte frames.

Cisco Catalyst 3550 Series switches

Beperking: VLAN-kaarten

Catalyst 3550 Series VLAN-kaarten kunnen worden geconfigureerd om MPLS-frames in een VLAN te filteren. In het volgende voorbeeld hebben kwetsbare apparaten interfaces in VLAN's 162 en 200. Die VLAN's zijn geconfigureerd om inkomende MPLS-frames te laten vallen in de Cisco Catalyst 3550 Series-switch die als afschermingsapparaat fungeert:

```
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
```

Beperken: MAC-toegangsgroepen

Catalyst 3550 Series MAC-toegangsgroepen kunnen filteren op een bepaalde EtherType-waarde. Ze kunnen worden gebruikt om frames te ontkennen met EtherType 0x847 of 0x848. De toegangsgroep moet worden toegepast op alle poorten in het uitzenddomein van het kwetsbare apparaat. De Cisco Catalyst 3550 **MAC access-groep** kan alleen worden toegepast in de inkomende richting (**in** trefwoord)

```
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
```

Identificatie: MAC-toegangsgroepen en VLAN-kaarten

De Cisco Catalyst 3550 Series **toont hardwaretellers met toegangslijsten en** geprivilegieerde EXEC-mode-opdracht en geeft één algemene teller weer voor frames die worden gedropt door MAC-toegangslijsten of VLAN-kaarten. Er is een aparte teller voor het totale aantal bytes dat door beide functies wordt gelaten vallen. In het onderstaande voorbeeld werden 268 frames verwijderd, wat in totaal 21.177 bytes bedroeg.

```
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 3750 Series switches

Beperking: VLAN-kaarten

Catalyst 3750 Series VLAN-kaarten kunnen worden geconfigureerd om MPLS-frames in een VLAN te filteren. In het volgende voorbeeld, heeft een kwetsbare apparaten één interface in VLAN 163. Cisco 3750 die fungeert als een screeningapparaat zal inkomende MPLS-frames op VLAN 163 laten vallen.

```
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
```

Beperken: MAC-toegangsgroepen

Catalyst 3750 Series MAC-toegangsgroepen kunnen filteren op een bepaalde EtherType-waarde en kunnen worden gebruikt om frames te ontkennen met EtherType 0x847 of 0x848. De toegangsgroep moet worden toegepast op alle poorten in het uitzenddomein van het kwetsbare apparaat.

```
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
```

Identificatie: MAC-toegangsgroepen en VLAN-kaarten

De Cisco Catalyst 3750 Series **toont hardwaretellers met** een geprivilegieerde EXEC-opdracht en geeft één algemene teller weer voor frames die worden gedropt door alle MAC-toegangsgroepen of VLAN-kaarten. Er is een afzonderlijke globale teller voor het totale aantal bytes die door beide eigenschappen worden gelaten vallen.

```
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 de vorige output, werden 18.170 frames door de toegangsgroepen van MAC of kaarten van VLAN gelaten vallen. Het totale aantal bytes in de gevallen frames was 2.999.815.

Cisco Catalyst 4500 Series switches

De voorgestelde beperking in de Cisco Catalyst 4500 Series is alleen mogelijk als alleen IP-frames zijn toegestaan door het beveiligingsbeleid. De implementatie van de **mac access-list** opdracht maakt het alleen mogelijk een vooraf gedefinieerde set protocollen te filteren. De voorgestelde beperking voor de Cisco Catalyst 6000- en 6500-serie en Cisco 7600 Series MPLS-pakketkwetsbaarheid zal onder andere AppleTalk- en IPX-frames laten vallen.

Beperking: VLAN-kaarten

Catalyst 4500 Series VLAN-kaarten bieden de mogelijkheid om te filteren volgens een vooraf gedefinieerde lijst met protocoltypen. Beperking van de pakketkwetsbaarheid van Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series MPLS kan worden bereikt door alle niet-IP-frames te filteren. In het volgende voorbeeld zal VLAN 160 alle niet-IP frames laten vallen om een kwetsbaar apparaat te beschermen dat een interface heeft in 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
```

Beperking: poortACL's

Catalyst 4500 Series ACL (ACL) met poorten kan de kwetsbaarheid van Cisco Catalyst 6000 en 6500 Series en Cisco 7600 Series MPLS-pakket verminderen. De PAL in de Cisco Catalyst 4500 Series kan in de inkomende of uitgaande richting worden toegepast. Het bevel van de de interfaceconfiguratie van de **toegangsgroepwijze** kan worden gebruikt om de interactie tussen het PACL, de kaart van VLAN, en routerACL te controleren die op de haven van toepassing zijn.

```
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
```

Houd er rekening mee dat de functies Cisco Catalyst 4500 Series VLAN-kaarten en -PAL IP-protocolframes die erdoor stromen, niet blokkeren (EtherTypes 0x0800 en 0x0806). De volgende frames, die door de switch zelf zijn verwerkt of gegenereerd, worden niet geblokkeerd:

- Spanning Tree 802.1d BPDU
- Cisco Shared Spanning Tree Protocol (SSTP)
- Cisco Discovery Protocol (CDP)
- Unidirectionele linkdetectie (UDLD)
- VLAN-trunkingprotocol (VTP)

Identificatie: VLAN-kaarten en -PAL

Catalyst 4500 Series implementeert tellers per MAC Access Control Entry (ACE). Houd er rekening mee dat de configuratie die vereist is om de Cisco Catalyst 6000- en 6500-serie en Cisco 7600 Series MPLS-pakketkwetsbaarheid te beperken, loopback-frames zou blokkeren (EtherType 0x9000). Er is geen operationele impact voor Catalyst 4500 Series om loopback frames van externe stations te laten vallen. Vanwege het laten vallen van loopback frames, zal het **show access-lists** geprivilegieerde EXEC mode commando voortdurend het aantal overeenkomende frames verhogen. De standaardinstelling in Cisco IOS-apparaten is om een loopback-frame elke 10 seconden te verzenden (**keepive** opdracht voor interfaceconfiguratie).

```
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 de voorbeelduitvoer, werden 1151 frames door de MAC ACL die door het voorbeeld PACL wordt gebruikt laten vallen en 820 frames werden door de steekproef VLAN kaartconfiguratie gelaten vallen.

Beperking: {Inhoud hier invoegen}

- Cisco Catalyst 6000 en 6500 Series VLAN-toegangslijsten (VACL's) bieden *geen* effectieve beperking. VACL's voorkomen niet dat MPLS-frames de routeprocessor bereiken, noch dat ze deze frames filteren voor upstream-apparaten.
- Cisco Catalyst 2950 Series implementatie van de MAC-toegangsgroepfunctie maakt het niet mogelijk geëtiketteerde pakketten onafhankelijk van IP-pakketten te filteren en kan niet worden gebruikt als een screeningapparaat voor de Cisco Catalyst 6000- en 6500-reeks en Cisco 7600 Series MPLS-pakketkwetsbaarheid.

Aanvullende informatie

DIT DOCUMENT WORDT AANGEBODEN OP EEN 'AS IS'-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIP VAN GARANTIES VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. UW GEBRUIK VAN DE INFORMATIE IN HET DOCUMENT OF DE MATERIALEN GEKOPPELD AAN HET DOCUMENT IS GEHEEL OP EIGEN RISICO. CISCO BEHOUDT ZICH HET RECHT VOOR OM DIT DOCUMENT TE ALLEN TIJDE TE WIJZIGEN OF TE ANNULEREN.

Revisiegeschiedenis

Revisie 1.0	2007-februari-28	Eerste publieke publicatie.

Cisco-beveiligingsprocedures

Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dit omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op http://www.cisco.com/go/psirt.

Gerelateerde informatie

- Cisco-bulletins voor toepassingsbeperking
- Cisco-beveiliging
- Cisco-handleiding over het versterken van Cisco IOS-apparaten
- De betekenis van cross-site scripting (XSS) bedreigingsvectoren
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- NetFlow-prestatieanalyse
- Witboeken voor Cisco Network Foundation-bescherming
- Presentaties voor Cisco Network Foundation-bescherming
- Identificatie en beperking van TTL-aanval bij verlopen
- Een security georiënteerde benadering van IP-adressering
- Tegenmaatregelen voor kwaadwillig gebruik van IPv6 Type 0-routingkoppen
- Inzicht in bescherming van besturingsplane
- Opdrachttaal voor gereedschap beveiligen op Cisco IOS
- Cisco Firewallproducten - startpagina op Cisco.com

- Voorkomen dat ActiveX wordt geëxploiteerd met Cisco Firewall Application Layer Inspection
- Voorkomen van ActiveX-exploitatie met Cisco Application Control Engine Application Layer Protocol Inspectie
- Cisco ACE-documentatie voor Application Control Engine
- Verbeteringen in Unicast Reverse Path Forwarding voor de Internet Service Provider
- Cisco 6.x inbraakpreventiesysteem
- Cisco IPS 6.x downloads voor handtekeningen
- Cisco-zoekpagina voor IPS-handtekeningen
- Cisco-systeem voor beveiligingsbewaking, analyse en respons
- Cisco Security Agent
- Gemeenschappelijke kwetsbaarheden en blootstellingen (CVE)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.