Cisco Catalyst 6000, 6500 및 Cisco 7600 Series MPLS 패킷 취약성 식별 및 완화

Cisco Catalyst 6000, 6500 및 Cisco 7600 Series MPLS 패킷 취약성 식별 및 완화

자문 ID: cisco-amb-20070228-mpls

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

개정 1.0

2007년 2월 28일 16:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

취약성 특성

Cisco Catalyst 6000 및 6500 Series 및 Cisco 7600 Series MPLS(Multiprotocol Label Switching) 패킷 취약성은 인증 없이 로컬 세그먼트에서 악용될 수 있으며 사용자 상호 작용은 필요하지 않습니다. 취약성으로 인해 DoS(denial of service) 조건이 발생할 수 있습니다. 공격 벡터는 MPLS 프레임(EtherType 0x8847 및 0x8848)을 통해 이루어집니다. 이 취약성은 CVE ID로 지정되지 않습니다.

이 문서에는 Cisco 고객이 Cisco Catalyst 6000 및 6500 Series 및 Cisco 7600 Series MPLS 패킷 취약성을 악용하려는 시도를 식별하고 완화하는 데 도움이 되는 정보가 포함되어 있습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어 및 고정 소프트웨어에 대한 정보는 PSIRT Security Advisory에서 확인할 수 있습니다.

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

완화 기법 개요

Cisco 디바이스는 Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series MPLS 패킷 취약성에 대한 몇 가지 대응책을 제공합니다. 이 문서에서는 스위치드 액세스 레이어 뒤의 코어 및 디스트리뷰션 레이어에 있는 취약한 Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series 시스템의 완화 방법을 중점적으로 살펴봅니다. 이 문서에 포함된 완화 및 식별 기법은 이러한 액세스 레이어 스위치에서 이 취약성을 악용하는 데 사용될 수 있는 프레임을 필터링하는 데 사용됩니다.

Cisco 네트워크 디바이스에서 제공하는 가장 예방적인 제어는 IOS VLAN 맵을 사용하는 것입니다.

Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series 시스템은 MPLS 프레임을 필터링하는 데 효과적이지 않습니다.

위험 관리

조직은 표준 위험 평가 및 완화 프로세스를 준수하여 [이 취약성|이러한 취약성]의 잠재적 영향을 확인하는 것이 좋습니다. 분류(Triage)란 성공 가능성이 가장 높은 프로젝트를 분류하고 노력을 우선순위를 정하는 것을 말한다. Cisco는 조직이 정보 보안 팀을 위해 위험 기반 분류 기능을 개발하는 데 도움이 될 문서를 제공했습니다. 보안 취약성 알림에 대한 위험 분류 및 위험 분류 및 프로토타이핑은 조직이 반복 가능한 보안 평가 및 대응 프로세스를 개발하는 데 도움이 될 수 있습니다.

디바이스별 완화 및 식별

완화 및 식별에 대한 구체적인 내용은 다음과 같습니다.

- Cisco IOS 스위치

Cisco IOS 스위치

주의: 모든 완화 기법의 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

MPLS 패킷 취약성을 완화하기 위해 Cisco Catalyst 6000, 6500 Series 및 7600 Series 시스템 앞에서 선별용 디바이스로 테스트된 Catalyst IOS Series 스위치 목록은 다음과 같습니다.

- Cisco Catalyst 2960 시리즈
- Cisco Catalyst 3550 시리즈
- Cisco Catalyst 3750 시리즈
- Cisco Catalyst 4500 시리즈

Cisco Catalyst 2960 Series Switches

완화: MAC 액세스 그룹

MAC 액세스 그룹을 사용하여 EtherType 0x8847 및 EtherType 0x8848 프레임이 포트에 들어가지 않도록 필터링할 수 있습니다. 완화가 유효하려면 MAC 액세스 그룹을 취약한 디바이스와 동일한 브로드캐스트 도메인의 모든 포트에 적용해야 합니다. Cisco Catalyst 2960 Series 스위치에서는 입력 방향(**in** 키워드)에 **mac 액세스 그룹만** 적용할 수 있습니다

```
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
```

ID: MAC 액세스 그룹

Cisco Catalyst 2960 Series **show access-lists hardware counters** privileged EXEC mode 명령은 모든 MAC 액세스 목록에 의해 삭제된 프레임에 대한 단일 전역 카운터("Drop: All frame count")와 삭제된 프레임에서 총 바이트 수에 대한 단일 전역 카운터("Drop: All bytes count")를 표시합니다

```
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
.
.
.
```

이 예에서는 스위치의 모든 MAC 액세스 그룹에서 165개 프레임이 삭제되었으며, 삭제된 165개 프레임 내에 총 19,684바이트가 포함되었습니다.

Cisco Catalyst 3550 Series Switches

완화: VLAN 맵

Catalyst 3550 Series VLAN 맵은 VLAN에서 MPLS 프레임을 필터링하도록 구성할 수 있습니다. 다음 예에서 취약한 디바이스는 VLAN 162 및 200에 인터페이스가 있습니다. 이러한 VLAN은 차폐 장치의 역할을 하는 Cisco Catalyst 3550 Series 스위치에서 들어오는 MPLS 프레임을 삭제하도록 구성됩니다.

```
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
```

완화: MAC 액세스 그룹

Catalyst 3550 Series MAC 액세스 그룹은 지정된 EtherType 값을 기준으로 필터링할 수 있습니다. 이더 타입 0x8847 또는 0x8848의 프레임을 거부하는 데 사용할 수 있습니다. 액세스 그룹은 취약한 디바이스의 브로드캐스트 도메인에 있는 모든 포트에 적용되어야 합니다. Cisco Catalyst 3550 **mac access-group은** 들어오는 방향에만 적용할 수 있습니다(in 키워드)

```
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
```

ID: MAC 액세스 그룹 및 VLAN 맵

Cisco Catalyst 3550 Series **show access-lists hardware counters** privileged EXEC mode 명령은 MAC 액세스 목록 또는 VLAN 맵에서 삭제된 프레임에 대한 단일 전역 카운터를 표시합니다. 두 기능 모두에서 삭제된 총 바이트 수에 대한 카운터가 별도로 있습니다. 아래 예에서는 268개의 프레임이 삭제되었으며, 이는 총 21,177바이트를 차지했습니다.

```
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

완화: VLAN 맵

Catalyst 3750 Series VLAN 맵은 VLAN에서 MPLS 프레임을 필터링하도록 구성할 수 있습니다. 다음 예에서 취약한 디바이스는 VLAN 163에 하나의 인터페이스가 있습니다. 스크리닝 디바이스 역할을 하는 Cisco 3750은 VLAN 163에서 들어오는 MPLS 프레임을 삭제합니다.

```
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
```

완화: MAC 액세스 그룹

Catalyst 3750 Series MAC 액세스 그룹은 지정된 EtherType 값을 필터링할 수 있으며, EtherType 0x8847 또는 0x8848의 프레임을 거부하는 데 사용할 수 있습니다. 액세스 그룹은 취약한 디바이스의 브로드캐스트 도메인에 있는 모든 포트에 적용되어야 합니다.

```
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
```

ID: MAC 액세스 그룹 및 VLAN 맵

Cisco Catalyst 3750 Series **show access-lists hardware counters** privileged EXEC mode 명령은 모든 MAC 액세스 그룹 또는 VLAN 맵에서 삭제된 프레임에 대한 단일 전역 카운터를 표시합니다. 두 기능 모두에서 삭제된 총 바이트 수에 대한 별도의 단일 전역 카운터가 있습니다.

```
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
.
.
.
```

이전 출력에서는 MAC 액세스 그룹 또는 VLAN 맵에서 18,170개의 프레임이 삭제되었습니다. 삭제된 프레임의 총 바이트 수는 2,999,815였습니다.

Cisco Catalyst 4500 Series Switches

Cisco Catalyst 4500 Series의 권장 완화 방법은 보안 정책에서 IP 프레임만 허용하는 경우에만 가능합니다. **mac access-list** 명령 **구현**은 미리 정의된 프로토콜 집합만 필터링하도록 허용합니다. Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series MPLS 패킷 취약성에 대해 제안된 완화로 인해 AppleTalk 및 IPX 프레임이 중단될 수 있습니다.

완화: VLAN 맵

Catalyst 4500 Series VLAN 맵은 미리 정의된 프로토콜 유형 목록에 따라 필터링하는 기능을 제공합니다. Cisco Catalyst 6000/6500 및 Cisco 7600 Series MPLS 패킷 취약성을 완화하려면 모든 비 IP 프레임을 필터링해야 합니다. 다음 예에서 VLAN 160은 모든 비 IP 프레임을 삭제하여 VLAN 160에 인터페이스가 있는 취약한 디바이스를 보호합니다.

```
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
```

완화: 포트 ACL

Catalyst 4500 Series 포트 ACL(PACL)은 Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series MPLS 패킷 취약성을 완화할 수 있습니다. Cisco Catalyst 4500 Series의 PACL은 수신 또는 발신 방향으로 적용할 수 있습니다. access-**group mode** interface 컨피그레이션 명령을 사용하여 포트에 적용되는 PACL, VLAN 맵, 라우터 ACL 간의 상호 작용을 제어할 수 있습니다.

```
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
```

Cisco Catalyst 4500 Series VLAN 맵과 PACL 기능은 IP 프로토콜 프레임 흐름을 차단하지 않습니다(EtherTypes 0x0800 및 0x0806). 또한 스위치 자체에서 처리하거나 생성하는 다음 프레임은 차단하지 않습니다.

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

ID: VLAN 맵 및 PACL

Catalyst 4500 Series는 MAC ACE(Access Control Entry)당 카운터를 구현합니다. Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series MPLS 패킷 취약성을 완화하기 위해 필요한 컨피그레이션은 루프백 프레임(EtherType 0x9000)을 차단합니다. Catalyst 4500 Series는 외부 스테이션의 루프백 프레임을 삭제하는 데 아무런 영향을 미치지 않습니다. 루프백 프레임 삭제로 인해 **show access-lists** privileged EXEC mode 명령은 일치하는 프레임 수를 지속적으로 증가시킵니다. Cisco IOS 디바이스의 기본값은 10초마다 루프백 프레임을 전송하는 것입니다(keepalive interface configuration 명령).

```
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)
```

예제 출력에서는 예제 PACL에서 사용한 MAC ACL에 의해 1151개 프레임이 삭제되었고 샘플 VLAN 맵 컨피그레이션에 의해 820개 프레임이 삭제되었습니다.

완화: {여기에 콘텐츠 삽입}

- Cisco Catalyst 6000 및 6500 Series VACL(VLAN Access List)은 효과적인 차단 기능을 제공하지 *않습니다*. VACL은 MPLS 프레임이 Route Processor에 도달하는 것을 막지 않으며 업스트림 디바이스를 위해 이러한 프레임을 필터링하지도 않습니다.
- MAC 액세스 그룹 기능의 Cisco Catalyst 2950 Series 구현에서는 레이블이 지정된 패킷을 IP 패킷과 독립적으로 필터링할 수 없으며 Cisco Catalyst 6000 및 6500 Series와 Cisco 7600 Series MPLS 패킷 취약성을 위한 스크리닝 디바이스로 사용할 수 없습니다.

추가 정보

개정 이력

개정 1.0	2007년 2월 28일	초기 공개 릴리스.

Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원 요청, Cisco의 보안 정보 수신을 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html)에서 확인할 수 있습니다. 여기에는 Cisco 보안 알림과 관련된 언론 문의에 대한 지침이 포함됩니다. 모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

관련 정보

- Cisco AppliedMitigation 게시판
- Cisco 보안
- Cisco IOS 디바이스를 강화하는 Cisco 가이드
- XSS(Cross-Site Scripting) 위협 벡터 이해
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)
- Cisco IOS NetFlow 백서
- NetFlow 성능 분석
- Cisco 네트워크 기반 보호 백서
- Cisco Network Foundation Protection 프레젠테이션
- TTL 만료 공격 식별 및 완화
- 보안 중심의 IP 주소 지정 방식
- IPv6 Type 0 라우팅 헤더의 악의적인 사용에 대한 대책
- 컨트롤 플레인 보호 이해
- Cisco IOS의 보안 툴 명령 언어
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- Cisco Firewall Application Layer Protocol Inspection으로 ActiveX 익스플로잇 방지
- Cisco Application Control Engine Application Layer Protocol Inspection으로 ActiveX 익스플로잇 방지
- Cisco ACE Application Control Engine 모듈 설명서
- 인터넷 서비스 공급자를 위한 유니캐스트 역방향 경로 전달 개선 사항
- Cisco 6.x 침입 방지 시스템
- Cisco IPS 6.x 서명 다운로드
- Cisco IPS 서명 검색 페이지
- Cisco 보안 모니터링, 분석 및 대응 시스템
- Cisco 보안 에이전트
- CVE(Common Vulnerabilities and Exposures)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.