

Cisco Unified Communications Manager의 여러 취약성 식별 및 완화

Cisco Unified Communications Manager의 여러 취약성 식별 및 완화

자문 ID: cisco-amb-20110427-cucm

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110427-cucm>

개정 1.1

2011년 4월 27일 16:00 UTC (GMT)

목차

[Cisco의 대응](#)

[디바이스별 완화 및 식별](#)

[추가 정보](#)

[개정 이력](#)

[Cisco 보안 절차](#)

[관련 정보](#)

Cisco의 대응

이 Applied Mitigation Bulletin은 Cisco Unified *Communications Manager*의 PSIRT Security Advisory *Multiple Vulnerabilities*에 대한 보조 문서이며 관리자가 Cisco 네트워크 장치에 구축할 수 있는 식별 및 완화 기술을 제공합니다.

취약성 특성

Cisco Unified Communications Manager에는 여러 취약점이 있습니다. 다음 하위 섹션에는 이러한 취약성이 요약되어 있습니다.

SIP(Session Initiation Protocol) Denial of Service 취약성: 이러한 취약성은 인증 없이 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이러한 취약성을 성공적으로 악용하면 DoS(서비스 거부) 상태가 발생할 수 있습니다.

익스플로잇을 위한 공격 벡터는 다음 프로토콜과 포트를 사용하는 패킷을 통해 이루어집니다.

- TCP 포트 5060을 사용하는 SIP
- TCP 포트 5061을 사용하는 SIP
- UDP 포트 5060을 사용하는 SIP

- UDP 포트 5061을 사용하는 SIP

공격자는 스푸핑된 패킷을 사용하여 이러한 취약성을 악용할 수 있습니다.

이러한 취약성에는 CVE 식별자 CVE-2011-1604, CVE-2011-1605 및 CVE-2011-1606이 할당되었습니다.

Cisco Unified Reporting Unauthorized File Upload Vulnerability(Cisco Unified Reporting 무단 파일 업로드 취약성): 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 원격 공격자가 악성 파일을 업로드할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 8443을 사용하는 HTTPS 패킷을 통해 이루어집니다.

이 취약성에는 CVE 식별자 CVE-2011-1607이 할당되었습니다.

다중 SQL 주입 취약점: 이러한 취약점은 인증 및 인증 없이, 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이러한 취약점을 성공적으로 악용하면 정보 공개가 가능하므로 공격자가 해당 디바이스에 대한 정보를 학습할 수 있습니다.

익스플로잇을 위한 공격 벡터는 다음 프로토콜과 포트를 사용하는 패킷을 통해 이루어집니다.

- TCP 포트 80을 사용하는 HTTP
- TCP 포트 443을 사용하는 HTTPS
- TCP 포트 8080을 사용하는 HTTP
- TCP 포트 8443을 사용하는 HTTPS

이러한 취약성에는 CVE 식별자 CVE-2011-1609 및 CVE-2011-1610이 할당되었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어, 그리고 고정된 소프트웨어에 대한 정보는 PSIRT Security Advisory에서 확인할 수 있습니다. PSIRT Security Advisory는 다음 링크에서 확인할 수 있습니다. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110427-cucm>

완화 기법 개요

Cisco 디바이스는 이러한 취약성에 대한 몇 가지 대응책을 제공합니다. 관리자는 이러한 보호 방법을 인프라 디바이스 및 네트워크를 이동하는 트래픽에 대한 일반적인 보안 모범 사례로 고려하는 것이 좋습니다. 이 문서에서는 이러한 기술에 대한 개요를 제공합니다.

Cisco IOS Software는 다음 방법을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다

- 트랜짓 액세스 제어 목록(tACL)
- 유니캐스트 RPF(Unicast Reverse Path Forwarding)
- IP 소스 가드(IPSG)

이러한 보호 메커니즘은 이러한 취약성을 악용하려는 패킷의 소스 IP 주소를 확인하고 필터링하고 삭제합니다.

유니캐스트 RPF의 올바른 구축 및 컨피그레이션은 스푸핑된 소스 IP 주소가 있는 패킷을 사용하는 공격에 대해 효과적인 보호 방법을 제공합니다. 유니캐스트 RPF는 가능한 한 모든 트래픽 소스에 가깝게 구축해야 합니다.

IPSG의 적절한 구축 및 구성은 액세스 레이어에서 스푸핑 공격을 효과적으로 방어합니다.

Cisco ASA 5500 Series Adaptive Security Appliance 및 Cisco Catalyst 6500용 FWSM(Firewall Services Module)에서도 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다.

- tACL
- 유니캐스트 RPF

이러한 보호 메커니즘은 이러한 취약성을 악용하려는 패킷의 소스 IP 주소를 확인하고 필터링하고 삭제합니다.

Cisco IPS(Intrusion Prevention System) 이벤트 작업을 효과적으로 사용하면 이러한 취약성을 악용하려는 공격에 대한 가시성과 차단 기능을 제공할 수 있습니다.

Cisco IOS NetFlow 레코드는 네트워크 기반 익스플로잇 시도에 대한 가시성을 제공할 수 있습니다.

Cisco IOS Software, Cisco ASA 및 FWSM 방화벽은 **show** 명령 출력에 표시된 syslog 메시지 및 카운터 값을 통해 가시성을 제공할 수 있습니다.

Cisco Security MARS(Monitoring, Analysis, and Response System) 어플라이언스는 사고, 쿼리 및 이벤트 보고를 통해 가시성을 제공할 수도 있습니다.

위험 관리

조직은 이러한 취약성의 잠재적 영향을 판단하기 위해 표준 위험 평가 및 완화 프로세스를 따르는 것이 좋습니다. 분류(Triage)란 성공 가능성이 가장 높은 프로젝트를 분류하고 노력을 우선 순위를 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

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.

완화 및 식별에 대한 구체적인 정보를 다음 장치에 사용할 수 있습니다.

- [Cisco IOS 라우터 및 스위치](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA 및 FWSM 방화벽](#)
- [Cisco 침입 방지 시스템](#)
- [Cisco 보안 모니터링, 분석 및 대응 시스템](#)

[Cisco IOS 라우터 및 스위치](#)

완화: 통과 액세스 제어 목록

인터넷 연결 지점, 파트너 및 공급업체 연결 지점 또는 VPN 연결 지점이 포함될 수 있는 인그레스 액세스 지점에서 네트워크로 들어오는 트래픽으로부터 네트워크를 보호하려면 관리자가 tACL(transit access control list)을 구축하여 정책 시행을 수행하는 것이 좋습니다. 관리자는 승인 받은 트래픽만 인그레스 액세스 포인트에서 네트워크에 들어가도록 명시적으로 허용하거나 기존 보안 정책 및 컨피그레이션에 따라 인증 받은 트래픽이 네트워크를 통과하도록 허용하여 tACL을 구성

할 수 있습니다. tACL 해결 방법은 공격이 신뢰할 수 있는 소스 주소에서 시작되는 경우 이러한 취약성에 대한 완벽한 보호를 제공할 수 없습니다.

tACL 정책은 영향을 받는 디바이스에 전송되는 TCP 및 UDP 포트 5060 및 5061의 무단 SIP 패킷, TCP 포트 80 및 8080의 HTTP 패킷, TCP 포트 443 및 8443의 HTTPS 패킷을 거부합니다. 다음 예에서 192.168.60.0/24은 영향을 받는 디바이스에서 사용하는 IP 주소 공간이며, 192.168.100.1의 호스트는 영향을 받는 디바이스에 액세스해야 하는 신뢰할 수 있는 소스로 간주됩니다. 모든 무단 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다.

tACL에 대한 추가 정보가 [트랜짓 액세스 제어 목록: 에지에서 필터링에 있습니다.](#)

```
!-- Include explicit permit statements for trusted sources !-- that require access on
the vulnerable ports ! access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 80 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 443 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 ! !--
The following vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
5060 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny
udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny udp any 192.168.60.0
0.0.0.255 eq 5061 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80 access-
list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 8080 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
8443 ! !-- 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 150 deny ip any any ! !-- Apply tACL to interfaces in the
ingress direction ! interface GigabitEthernet0/0 ip access-group 150 in
```

인터페이스 액세스 목록으로 필터링하면 ICMP 도달 불가 메시지를 필터링된 트래픽의 소스로 다시 전송합니다. 이러한 메시지를 생성하면 디바이스에서 CPU 사용률이 증가하는 원치 않는 영향을 미칠 수 있습니다. Cisco IOS Software에서 ICMP 연결 불가능 생성은 기본적으로 500밀리초마다 하나의 패킷으로 제한됩니다. ICMP 연결 불가 메시지 생성은 인터페이스 컨피그레이션 명령 `no ip unreachable`을 사용하여 비활성화할 수 있습니다. ICMP 연결 불가능 속도 제한은 `ip icmp rate-limit unreachable interval-in-ms` 전역 구성 명령을 사용하여 기본값에서 변경할 수 있습니다.

완화: 스푸핑 보호

유니캐스트 역방향 경로 전달

이 문서에 설명된 취약성은 스푸핑된 IP 패킷으로 악용될 수 있습니다. 관리자는 스푸핑에 대한 보호 메커니즘으로 유니캐스트 RPF(Unicast Reverse Path Forwarding)를 구축하고 구성할 수 있습니다.

유니캐스트 RPF는 인터페이스 레벨에서 구성되며 확인 가능한 소스 IP 주소가 없는 패킷을 탐지하고 삭제할 수 있습니다. 관리자는 소스 IP 주소에 대한 적절한 반환 경로가 있는 경우 스푸핑된 패킷이 유니캐스트 RPF 지원 인터페이스를 통해 네트워크에 진입할 수 있으므로 완벽한 스푸핑 보호를 제공하기 위해 유니캐스트 RPF에 의존해서는 안 됩니다. 이 기능은 네트워크를 통과하는 합법적인 트래픽을 삭제할 수 있으므로 관리자는 이 기능을 구축하는 동안 적절한 유니캐스트 RPF 모드(느슨하거나 엄격함)가 구성되었는지 확인하는 것이 좋습니다. 엔터프라이즈 환경에서는 인터넷 에지와 사용자 지원 레이어 3 인터페이스의 내부 액세스 레이어에서 유니캐스트 RPF가 활성화될 수 있

습니다.

추가 정보는 Unicast [Reverse Path Forwarding Loose Mode 기능 가이드에 있습니다.](#)

유니캐스트 RPF의 컨피그레이션 및 사용에 대한 자세한 내용은 Understanding Unicast [Reverse Path Forwarding Applied](#) Intelligence 백서를 참조하십시오.

IP Source Guard

IPSG(IP source guard)는 DHCP 스누핑 바인딩 데이터베이스 및 수동으로 구성된 IP 소스 바인딩을 기반으로 패킷을 필터링하여 라우팅되지 않은 레이어 2 인터페이스의 IP 트래픽을 제한하는 보안 기능입니다. 관리자는 IPSG를 사용하여 소스 IP 주소 및/또는 MAC 주소를 위조하여 패킷을 스누핑하려고 시도하는 공격자의 공격을 방지할 수 있습니다. IPSG를 올바르게 구축하고 구성하면 엄격한 모드 유니캐스트 RPF와 결합하여 이 문서에 설명된 취약성에 대한 가장 효과적인 스누핑 보호 방법을 제공합니다.

IPSG 구축 및 컨피그레이션에 대한 추가 정보는 DHCP 기능 [및 IP 소스การ์ด 구성에 있습니다.](#)

식별: 통과 액세스 제어 목록

관리자가 인터페이스에 tACL을 적용한 후 **show ip access-lists** 명령은 필터링된 TCP 및 UDP 포트 5060 및 5061의 SIP 패킷, TCP 포트 80 및 8080의 HTTP 패킷, TCP 포트 443 및 8443의 HTTPS 패킷 수를 식별합니다. 관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인하는 것이 좋습니다. **show ip access-lists 150**에 대한 **출력의 예**는 다음과 같습니다.

```
router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
 20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
 30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
 40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
 50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
 60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
 70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
 80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
 90 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (17 matches)
100 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (19 matches)
110 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (3 matches)
120 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (49 matches)
130 deny tcp any 192.168.60.0 0.0.0.255 eq 80 (32 matches)
140 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (20 matches)
150 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (35 matches)
160 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (10 matches)
170 deny ip any any
```

router#

앞의 예에서 액세스 목록 150은 신뢰할 수 없는 호스트 또는 네트워크로부터 수신한 다음 패킷을 삭제했습니다.

- ACE 라인 90에 대한 TCP 포트 5060의 SIP 패킷 17개
- ACE 라인 100에 대한 TCP 포트 5061의 SIP 패킷 19개
- ACE 라인 110에 대한 UDP 포트 5060의 SIP 패킷 3개
- ACE 라인 120에 대한 UDP 포트 5061의 SIP 패킷 49개
- ACE 라인 130에 대한 TCP 포트 80의 32개 HTTP 패킷
- ACE 라인 140에 대한 TCP 포트 443의 20개 HTTPS 패킷

- ACE 라인 150에 대한 TCP 포트 8080의 35개 HTTP 패킷
- ACE 라인 160에 대한 TCP 포트 8443의 HTTPS 패킷 10개

ACE 카운터 및 syslog 이벤트를 사용한 인시던트 조사에 대한 자세한 내용은 [Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence](#) 백서를 참조하십시오.

관리자는 ACE 카운터 적중과 같은 특정 조건이 충족될 때 Embedded Event Manager를 사용하여 계측을 제공할 수 있습니다. [보안](#) 컨텍스트의 Embedded [Event Manager](#) Applied Intelligence [백서](#)에서는 이 기능 사용 방법에 대한 추가 세부 정보를 제공합니다.

ID: 액세스 목록 로깅

log and **log-input** ACL(access control list) 옵션을 사용하면 특정 ACE와 일치하는 패킷이 로깅됩니다. **log-input** 옵션은 패킷 소스 및 목적지 IP 주소와 포트 외에 인그레스 인터페이스의 로깅을 활성화합니다.

주의: 액세스 제어 목록 로깅은 CPU를 많이 사용할 수 있으므로 각별한 주의를 기울여 사용해야 합니다. ACL 로깅의 CPU 영향을 제어하는 요소는 로그 생성, 로그 전송, 로그 지원 ACE와 일치하는 패킷을 전달하는 프로세스 스위칭입니다.

Cisco IOS Software의 경우 **ip access-list logging interval in-ms** 명령은 ACL 로깅에 의해 유발되는 프로세스 전환의 효과를 제한할 수 있습니다. **logging rate-limit rate-per-second [except loglevel]** 명령은 로그 생성 및 전송의 영향을 제한합니다.

ACL 로깅의 CPU 영향은 Supervisor Engine 720 또는 Supervisor Engine 32를 사용하는 Cisco Catalyst 6500 Series 스위치와 Cisco 7600 Series 라우터의 하드웨어에서 최적화된 ACL 로깅을 사용하여 해결할 수 있습니다.

ACL 로깅의 컨피그레이션 및 사용에 대한 자세한 내용은 ACL [로깅 적용 인텔리전스 이해](#) 백서를 참조하십시오.

식별: 유니캐스트 역방향 경로 전달을 사용하는 스푸핑 보호

네트워크 인프라 전체에 유니캐스트 RPF가 올바르게 배포 및 구성된 경우 관리자는 **show cef interface type slot/port internal**, **show ip interface**, **show cef drop**, **show ip cef switching statistics** 기능 및 **show ip traffic** 명령을 사용하여 유니캐스트 RPF가 삭제한 패킷 수를 식별할 수 있습니다.

참고: Cisco IOS Software 버전 12.4(20)T부터 **show ip cef switching** 명령이 **show ip cef switching statistics** 기능으로 대체되었습니다.

참고: **show** 명령은 **| regex 시작** 및 **show 명령 | include regex** 명령 수정자는 다음 예에서 사용되므로 원하는 정보를 보기 위해 관리자가 구문 분석해야 하는 출력의 양을 최소화합니다. 명령 수정자에 대한 자세한 내용은 Cisco [IOS](#) Configuration Fundamentals 명령 참조의 **show** 명령 섹션에 있습니다.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
```

```
ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

참고: **show cef interface type slot/port internal**은 CLI에서 완전히 입력해야 하는 숨겨진 명령입니다. 명령 완료를 사용할 수 없습니다.


```
router#show ip interface GigabitEthernet 0/0 | begin verify
```

```
IP verify source reachable-via RX, allow default, allow self-ping
18 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            18        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                18    0        0      0        0
Total                18    0        0      0        0
--      CLI Output Truncated  --
router#
```

```
router#show ip traffic | include RPF
```

```
18 no route, 18 unicast RPF, 0 forced drop
```

```
router#
```

앞의 show cef drop, show ip cef switching statistics feature 및 show ip traffic 예시에서 Unicast RPF는 Cisco Express Forwarding의 Forwarding Information Base 내에서 IP 패킷의 소스 주소를 확인할 수 없기 때문에 유니캐스트 RPF가 구성된 모든 인터페이스에서 전역적으로 수신한 18개 IP 패킷을 삭제했습니다.

[Cisco IOS NetFlow](#)

식별: NetFlow 레코드를 사용한 트래픽 흐름 식별

관리자는 Cisco IOS 라우터 및 스위치에서 Cisco IOS NetFlow를 구성하여 이러한 취약성을 악용하려는 시도일 수 있는 트래픽 흐름을 식별할 수 있도록 지원할 수 있습니다. 관리자는 플로우를 조사하여 이러한 취약성을 악용하려는 시도인지 또는 올바른 트래픽 플로우인지 확인하는 것이 좋습니다.

```
router#show ip cache flow
```

```
IP packet size distribution (31715553 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .005 .175 .632 .032 .095 .003 .003 .003 .002 .000 .005 .002 .000 .000 .000

 512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .020 .007 .008 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456704 bytes
```

```
24 active, 65512 inactive, 5451612 added
557541771 aged polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
```

```
IP Sub Flow Cache, 533256 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	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	811	0.0	137	41	0.0	32.3	16.4
TCP-FTP	2108	0.0	6	44	0.0	0.5	22.1
TCP-FTPD	5	0.0	13	52	0.0	0.7	1.5
TCP-WWW	133468	0.0	4	223	0.1	5.5	50.9
TCP-SMTP	32583	0.0	5	60	0.0	28.3	60.0
TCP-other	627608	0.1	12	175	1.8	57.8	24.1
UDP-DNS	284078	0.0	3	63	0.2	15.1	53.5
UDP-NTP	94456	0.0	1	76	0.0	0.3	60.5
UDP-Frag	1	0.0	9	1260	0.0	0.4	60.2
UDP-other	1102669	0.2	8	102	2.1	34.3	47.5
ICMP	1980458	0.4	2	89	1.1	14.3	58.5
IGMP	469264	0.1	2	37	0.2	58.2	41.0
IPINIP	2	0.0	1	76	0.0	0.0	60.4
IPv6INIP	3	0.0	1	863	0.0	0.0	60.4
GRE	2	0.0	1	697	0.0	0.0	60.4
IP-other	724037	0.1	9	89	1.5	95.0	15.6
Total:	5451553	1.2	5	113	7.3	37.5	44.7

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	1
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	13C5	3
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.13.97	Gi0/1	192.168.60.28	11	0B3E	13C4	5
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	06	0B89	13C4	1
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.12.185	Gi0/1	192.168.60.239	11	0BD7	13C4	1
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1
Gi0/0	192.168.120.20	Gi0/1	192.168.60.102	06	0984	1F90	1
Gi0/0	192.168.12.45	Gi0/1	192.168.60.138	06	0911	13C5	3
Gi0/1	192.168.150.41	Gi0/0	192.168.60.24	06	0016	12CA	1
Gi0/0	192.168.12.87	Gi0/1	192.168.60.28	06	0B3E	0050	5
Gi0/0	192.168.10.12	Gi0/1	192.168.60.97	06	0B89	01BB	1
Gi0/0	10.88.226.8	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.12.15	Gi0/1	192.168.60.209	06	0BD7	20FB	1
Gi0/0	10.89.16.216	Gi0/1	192.168.150.8	06	12CA	0016	1

router#

앞의 예에서는 TCP 포트 5060(16진수 값 13C4) 및 5061(16진수 값 13C5)의 SIP 및 UDP 포트 5060(13C4) 및 5061(16진수 값 13C5)의 HTTP 및 TCP 포트 80(16진수 값 0050) 및 8080(16진수 값 1F90)의 HTTP 및 TCP 포트 443(16진수 값 01BB) 및 843(16진수 20FB)의 HTTPS 여러 플로우가 있습니다.

이 트래픽은 영향을 받는 디바이스에서 사용하는 192.168.60.0/24 주소 블록 내의 주소에서 소싱되어 해당 주소로 전송됩니다. 이러한 흐름의 패킷은 스푸핑될 수 있으며, 이러한 취약성을 악용하려는 시도를 나타낼 수 있습니다. 관리자는 이러한 플로우를 UDP 포트 5060 및 포트 5061에서 전송된 SIP 트래픽의 기존 사용률과 비교하고, 플로우가 신뢰할 수 없는 호스트 또는 네트워크에서 소싱되는지 여부를 확인하는 것이 좋습니다.

UDP 포트 5060(16진수 값 13C4) 및 5061(16진수 값 13C5)에서 SIP 패킷에 대한 트래픽 흐름만 보려면 명령 `show ip cache flow | include SrcIf_11_.*(13C4|13C5)`는 다음과 같이 관련 UDP NetFlow 레코드를 표시합니다.

UDP 플로우


```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.12.110	Gi0/1	192.168.60.163	11	092A	13C4	6
Gi0/0	192.168.11.230	Gi0/1	192.168.60.20	11	0C09	13C4	1
Gi0/0	192.168.11.131	Gi0/1	192.168.60.245	11	0B66	13C5	18
Gi0/0	192.168.13.7	Gi0/1	192.168.60.162	11	0914	13C4	1

```
router#
```

TCP 포트 5060(16진수 값 13C4) 및 5061(16진수 값 13C5)의 SIP 패킷과 TCP 포트 80(16진수 값 0050) 및 8080(16진수 값 1F90)의 HTTP 패킷 및 TCP 포트 443(16진수 값 01BB) 및 8443(16진수 값 20FB)의 HTTPS 패킷에 대한 트래픽 흐름만 보려면 명령에서 ip 캐시 흐름을 표시합니다 | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB)는 다음과 같이 관련 TCP NetFlow 레코드를 표시합니다.

TCP 흐름

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB)
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.12.110	Gi0/1	192.168.60.163	06	092A	13C5	6
Gi0/0	192.168.11.230	Gi0/1	192.168.60.20	06	0C09	0050	1
Gi0/0	192.168.11.131	Gi0/1	192.168.60.245	06	0B66	01BB	18
Gi0/0	192.168.13.7	Gi0/1	192.168.60.162	06	0914	0050	7
Gi0/0	192.168.241.106	Gi0/1	192.168.60.27	06	0B7B	13C4	12
Gi0/0	192.168.19.222	Gi0/1	192.168.60.120	06	0C09	20FB	16
Gi0/0	192.168.12.121	Gi0/1	192.168.60.245	06	0B66	01BB	19
Gi0/0	192.168.14.17	Gi0/1	192.168.60.183	06	0914	1F90	9
Gi0/0	192.168.41.86	Gi0/1	192.168.60.217	06	0B7B	20FB	2

```
router#
```

Cisco ASA 및 FWSM 방화벽

완화: 통과 액세스 제어 목록

인터넷 연결 지점, 파트너 및 공급업체 연결 지점 또는 VPN 연결 지점이 포함될 수 있는 인그레스 액세스 지점에서 네트워크로 들어오는 트래픽으로부터 네트워크를 보호하려면 관리자가 tACL을 구축하여 정책 적용을 수행하는 것이 좋습니다. 관리자는 승인 받은 트래픽만 인그레스 액세스 포인트에서 네트워크에 들어가도록 명시적으로 허용하거나 기존 보안 정책 및 컨피그레이션에 따라 인증 받은 트래픽이 네트워크를 통과하도록 허용하여 tACL을 구성할 수 있습니다. tACL 해결 방법은 공격이 신뢰할 수 있는 소스 주소에서 시작되는 경우 이러한 취약성에 대한 완벽한 보호를 제공할 수 없습니다.

tACL 정책은 영향을 받는 디바이스에 전송되는 TCP 및 UDP 포트 5060 및 5061의 무단 SIP 패킷, TCP 포트 80 및 8080의 HTTP 패킷, TCP 포트 443 및 8443의 HTTPS 패킷을 거부합니다. 다음 예에서 192.168.60.0/24은 영향을 받는 디바이스에서 사용하는 IP 주소 공간이며, 192.168.100.1의 호스트는 영향을 받는 디바이스에 액세스해야 하는 신뢰할 수 있는 소스로 간주됩니다. 모든 무단 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다.

tACL에 대한 추가 정보가 [트랜짓 액세스 제어 목록: 예지에서 필터링에 있습니다.](#)

```
!!-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable ports ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq sip
```

```

access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8080 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 ! !-
- The following vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny udp any
192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended deny udp any
192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq www access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 ! !-- 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

```

완화: 유니캐스트 역방향 경로 전달을 사용한 스푸핑 보호

이 문서에 설명된 취약성은 스푸핑된 IP 패킷으로 악용될 수 있습니다. 관리자는 스푸핑에 대한 보호 메커니즘으로 유니캐스트 RPF를 구축하고 구성할 수 있습니다.

유니캐스트 RPF는 인터페이스 레벨에서 구성되며 확인 가능한 소스 IP 주소가 없는 패킷을 탐지하고 삭제할 수 있습니다. 관리자는 소스 IP 주소에 대한 적절한 반환 경로가 있는 경우 스푸핑된 패킷이 유니캐스트 RPF 지원 인터페이스를 통해 네트워크에 진입할 수 있으므로 완벽한 스푸핑 보호를 제공하기 위해 유니캐스트 RPF에 의존해서는 안 됩니다. 엔터프라이즈 환경에서는 인터넷 에지와 사용자 지원 레이어 3 인터페이스의 내부 액세스 레이어에서 유니캐스트 RPF가 활성화될 수 있습니다.

유니캐스트 RPF의 컨피그레이션 및 사용에 대한 자세한 내용은 Cisco Security Appliance Command Reference for [ip verify reverse-path](#) 및 Understanding Unicast [Reverse Path Forwarding Applied](#) Intelligence 백서를 참조하십시오.

식별: 통과 액세스 제어 목록

인터페이스에 tACL이 적용되면 관리자는 **show access-list** 명령을 사용하여 필터링된 TCP 및 UDP 포트 5060 및 5061의 SIP 패킷, TCP 포트 80 및 8080의 HTTP 패킷, TCP 포트 443 및 8443의 HTTPS 패킷 수를 식별할 수 있습니다. 관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인하는 것이 좋습니다. **show access-list tACL-Policy**의 출력 예는 다음과 같습니다.

```

firewall#show access-list tACL-Policy
access-list tACL-Policy; 17 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.60.0

```

```

255.255.255.0 eq www
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq https
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8443
access-list tACL-Policy line 9 extended deny tcp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=30)
access-list tACL-Policy line 10 extended deny tcp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=43)
access-list tACL-Policy line 11 extended deny udp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=70)
access-list tACL-Policy line 12 extended deny udp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=14)
access-list tACL-Policy line 13 extended deny tcp any 192.168.60.0 255.255.255.0 eq
www (hitcnt=45)
access-list tACL-Policy line 14 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=53)
access-list tACL-Policy line 15 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8080 (hitcnt=70)
access-list tACL-Policy line 16 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8443 (hitcnt=61)
access-list tACL-Policy line 17 extended deny tcp any any

```

앞의 예에서 액세스 목록 tACL-Policy는 신뢰할 수 없는 호스트 또는 네트워크에서 받은 다음 패킷을 삭제했습니다.

- ACE 라인 9의 TCP 포트 5060에서 30개 SIP 패킷
- ACE 라인 10에 대한 TCP 포트 5061의 SIP 패킷 43개
- ACE 라인 11용 UDP 포트 5060의 SIP 패킷 70개
- ACE 라인 12에 대한 UDP 포트 5061의 SIP 패킷 14개
- ACE 라인 13에 대한 TCP 포트 80의 45개 HTTP 패킷
- ACE 라인 14에 대한 TCP 포트 443의 53개 HTTPS 패킷
- ACE 라인 15에 대한 TCP 포트 8080에서 70개 HTTP 패킷
- ACE 라인 16에 대한 TCP 포트 8443의 61개 HTTPS 패킷

식별: 방화벽 액세스 목록 Syslog 메시지

log 키워드가 없는 ACE(Access Control Entry)에서 거부된 패킷에 대해 방화벽 syslog 메시지 **106023**이 생성됩니다. 이 syslog 메시지에 대한 추가 정보는 [Cisco ASA 5500 Series System Log Message, 8.2 - 106023에 있습니다.](#)

Cisco ASA 5500 Series Adaptive Security Appliance용 syslog 구성에 대한 정보는 [Monitoring - Configuring Logging에 있습니다.](#) Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 [Monitoring the Firewall Services Module에 있습니다.](#)

다음 예에서는 `show logging | grep regex` 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 이 문서에 설명된 취약성을 악용하려는 잠재적 시도를 나타낼 수 있는 거부된 패킷에 대한 추가 정보를 제공합니다. 로깅된 메시지에서 특정 데이터를 검색하기 위해 `grep` 키워드와 다른 정규식을 사용할 수 있습니다.

정규식 구문에 대한 추가 정보는 정규식 [만들기에 있습니다.](#)

```
firewall#show logging | grep 106023
```

```
Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.18/16784
```

```

dst inside:192.168.60.191/5060 by access-group "tACL-Policy"
Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.200/16785
dst inside:192.168.60.33/5060 by access-group "tACL-Policy"
Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.99/16786
dst inside:192.168.60.240/5061 by access-group "tACL-Policy"
Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.100/16787
dst inside:192.168.60.115/5061 by access-group "tACL-Policy"
Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.88/18683
dst inside:192.168.60.38/5060 by access-group "tACL-Policy"
Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.175/18684
dst inside:192.168.60.250/5061 by access-group "tACL-Policy"

```

firewall#

앞의 예에서 tACL tACL 정책에 대해 로깅된 메시지는 영향을 받는 디바이스에 할당된 주소 블록으로 전송된 TCP 및 UDP 포트(5060, 5061)에 대해 스푸핑된 SIP 패킷을 보여줍니다.

ASA 보안 어플라이언스용 syslog 메시지에 대한 추가 정보는 [Cisco ASA 5500 Series System Log Messages, 8.2에 있습니다](#). FWSM용 syslog 메시지에 대한 추가 정보는 [Catalyst 6500 Series Switch 및 Cisco 7600 Series Router Firewall Services Module Logging System Log Messages에 있습니다](#).

syslog 이벤트를 사용한 인시던트 조사에 대한 자세한 내용은 [Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence](#) 백서를 참조하십시오.

식별: 유니캐스트 역방향 경로 전달을 사용하는 스푸핑 보호

유니캐스트 RPF에서 거부된 패킷에 대해 방화벽 syslog 메시지 106021이 생성됩니다. 이 syslog 메시지에 대한 추가 정보는 [Cisco ASA 5500 Series System Log Message, 8.2 - 106021에 있습니다](#).

Cisco ASA 5500 Series Adaptive Security Appliance용 syslog 구성에 대한 정보는 [Monitoring - Configuring Logging에 있습니다](#). Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 [Monitoring the Firewall Services Module에 있습니다](#).

다음 예에서는 `show logging | grep regex` 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 이 문서에 설명된 취약성을 악용하려는 잠재적 시도를 나타낼 수 있는 거부된 패킷에 대한 추가 정보를 제공합니다. 로깅된 메시지에서 특정 데이터를 검색하기 위해 `grep` 키워드와 다른 정규식을 사용할 수 있습니다.

정규식 구문에 대한 추가 정보는 정규식 [만들기에 있습니다](#).

```
firewall#show logging | grep 106021
```

```

Apr 27 2011 00:03:42: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside
Apr 27 2011 00:03:43: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside
Apr 27 2011 00:03:43: %ASA-1-106021: Deny TCP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside

```

다음 예와 같이 `show asp drop` 명령은 유니캐스트 RPF 기능이 삭제한 패킷의 수를 식별할 수도 있습니다.

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

11

firewall#

앞의 예에서 Unicast RPF는 Unicast RPF가 구성된 인터페이스에서 수신된 11개의 IP 패킷을 삭제

했습니다. 출력이 없으면 방화벽의 유니캐스트 RPF 기능에서 패킷을 삭제하지 않았음을 나타냅니다.

가속화된 보안 경로 삭제 패킷 또는 연결 디버깅에 대한 자세한 내용은 Cisco Security Appliance Command Reference for [show asp drop](#)을 참조하십시오.

Cisco 침입 방지 시스템

완화: Cisco IPS 서명 이벤트 작업

관리자는 Cisco IPS(Intrusion Prevention System) 어플라이언스 및 서비스 모듈을 사용하여 위협 탐지를 제공하고 이 문서에 설명된 일부 취약성을 악용하려는 시도를 방지할 수 있습니다. 이러한 취약성은 다음 서명에 의해 탐지될 수 있습니다.

- 35846-0 - Cisco CUCM 원격 코드 실행
- 35866-0 - Cisco CUCM SIP 취약성
- 35085-0 - Cisco Call Manager SQL 삽입

35846-0 - Cisco CUCM 원격 코드 실행

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S562부터 시그니처 35846/0(시그니처 이름: Cisco CUCM Remote Code Execution)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 35846/0은 기본적으로 활성화되어 높은 심각도 이벤트를 트리거하고 SFR(Signature Fidelity Rating)이 95이며 **produce-alert**의 기본 이벤트 작업으로 구성됩니다.

서명 35846/0은 SIP 포트 5060을 사용하여 전송된 단일 패킷이 탐지될 때 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

35866-0 - Cisco CUCM SIP 취약성

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S562부터 시그니처 35866/0(시그니처 이름: Cisco CUCM SIP Vulnerability)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 35866/0은 기본적으로 활성화되어 높은 심각도 이벤트를 트리거하고 SFR(Signature Fidelity Rating)이 90이며 기본 이벤트 작업인 **produce-alert**로 구성됩니다.

서명 35866/0은 SIP 포트 5060을 사용하여 전송된 단일 패킷이 탐지될 때 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

35085-0 - Cisco Call Manager SQL 삽입

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S562부터 시그니처 35085/0(시그니처 이름: Cisco Call Manager SQL Injection)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 35085/0은 기본적으로 활성화되어 높은 심각도 이벤트를 트리거하고 SFR(Signature Fidelity Rating)이 85이며 기본 이벤트 작업인 **produce-alert**로 구성됩니다.

시그니처 35085/0은 Cisco의 Call Manager에 대한 SQL 삽입 공격을 탐지할 때 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

관리자는 공격이 탐지될 때 이벤트 작업을 수행하도록 Cisco IPS 센서를 구성할 수 있습니다. 구성된 이벤트 작업은 이 문서에 설명된 취약성을 악용하려는 공격으로부터 보호하기 위해 예방 또는 억제 제어를 수행합니다.

스푸핑된 IP 주소를 사용하는 익스플로잇은 구성된 이벤트 작업으로 인해 신뢰할 수 있는 소스의 트래픽을 실수로 거부할 수 있습니다.

Cisco IPS 센서는 이벤트 동작의 사용과 결합된 인라인 보호 모드에서 구축될 때 가장 효과적입니다. 인라인 보호 모드에서 구축된 Automatic Threat Prevention for Cisco IPS 6.x 이상 센서는 이 문서에 설명된 취약성을 악용하려는 공격에 대한 위협 방지 기능을 제공합니다. 위협 방지는 riskRatingValue가 90보다 큰 트리거된 서명에 대해 이벤트 작업을 수행하는 **기본 재정의**를 통해 구현됩니다.

위험 등급 및 위험 등급 계산에 대한 자세한 내용은 [위험 등급 및 위험 등급: IPS 정책 관리 간소화를 참조하십시오.](#)

[Cisco 보안 모니터링, 분석 및 대응 시스템](#)

식별: Cisco 보안 모니터링, 분석 및 대응 시스템 사고

Cisco Security MARS(Cisco Security Monitoring, Analysis, and Response System) 어플라이언스는 IPS 서명 35846/0(서명 이름: Cisco CUCM Remote Code Execution), IPS 서명 35866/0(서명 이름: Cisco CUCM SIP Vulnerability) 및 IPS 서명 35085/0(서명 이름: Cisco Call Manager SQL Injection)을 사용하여 이 문서에 설명된 취약성과 관련된 이벤트와 관련된 인시던트를 생성할 수 있습니다. S562 동적 서명 업데이트가 다운로드된 후 키워드 **NR-35846/0** for IPS signature 35846/0, 키워드 **NR-35866/0** for IPS signature 35866/0 또는 키워드 **NR-35085/0** for IPS signature 35085/0을 사용하여 Cisco Security MARS 어플라이언스에서 **모든 일치 이벤트의** 쿼리 유형에서 IPS 서명으로 생성된 인시던트를 나열하는 보고서를 제공합니다.

Cisco Security MARS 어플라이언스의 4.3.1 및 5.3.1 릴리스부터 Cisco IPS 동적 서명 업데이트 기능에 대한 지원이 추가되었습니다. 이 기능은 Cisco.com 또는 로컬 웹 서버에서 새 서명을 다운로드하고, 해당 서명과 일치하는 수신된 이벤트를 정확하게 처리 및 분류하며, 이를 검사 규칙 및 보고서에 포함합니다. 이러한 업데이트는 이벤트 표준화 및 이벤트 그룹 매핑을 제공하며 MARS 어플라이언스에서 IPS 디바이스의 새 서명을 구문 분석할 수 있게 합니다.

주의: 동적 서명 업데이트가 구성되지 않은 경우 이러한 새 서명과 일치하는 이벤트는 쿼리와 보고서에서 **알 수 없는 이벤트** 유형으로 표시됩니다. MARS는 이러한 이벤트를 검사 규칙에 포함하지 않으므로 네트워크 내에서 발생하는 잠재적인 위협이나 공격에 대한 인시던트가 생성되지 않을 수 있습니다.

기본적으로 이 기능은 활성화되어 있지만 컨피그레이션이 필요합니다. 구성되지 않은 경우 다음 Cisco 보안 MARS 규칙이 트리거됩니다.

System Rule: CS-MARS IPS Signature Update Failure

이 기능을 활성화하고 구성하면 관리자는 **도움말 > 정보**를 선택하고 **IPS 서명 버전 값을** 검토하여 MARS에서 다운로드한 현재 서명 버전을 결정할 수 있습니다.

동적 서명 업데이트에 대한 추가 정보 및 동적 서명 업데이트 구성에 대한 지침은 Cisco Security MARS [4.3.1](#) 및 [5.3.1 릴리스](#)에 제공됩니다.

추가 정보

이 문서는 "있는 그대로" 제공되며, 상품성 또는 특정 사용에 대한 적합성의 보증을 포함하여 어떤 종류의 보장 또는 보증도 의미하지 않습니다. 문서 또는 문서에 링크된 자료의 정보를 사용하는 것

은 귀하의 책임입니다. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

개정 이력

개정 1.1	2011년 4월 27일	IPS 시그니처 및 Cisco Security MARS에 대한 정보를 포함하도록 업데이트되었습니다.
개정 1.0	2011년 4월 27일	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/psirt>에서 확인할 수 [있습니다](#).

관련 정보

- [Cisco Applied Mitigation 게시판](#)
- [Cisco 보안](#)
- [Cisco Security IntelliShield Alert Manager Service](#)
- [Cisco IOS 디바이스를 강화하는 Cisco 가이드](#)
- [Cisco IOS NetFlow - 홈 페이지\(Cisco.com\)](#)
- [Cisco IOS NetFlow 백서](#)
- [NetFlow 성능 분석](#)
- [Cisco 네트워크 기반 보호 백서](#)
- [Cisco Network Foundation Protection 프레젠테이션](#)
- [보안 중심의 IP 주소 지정 방식](#)
- [Cisco 방화벽 제품 - 홈 페이지 Cisco.com](#)
- [인터넷 서비스 공급자를 위한 유니캐스트 역방향 경로 전달 개선 사항](#)
- [Cisco 침입 방지 시스템](#)
- [Cisco IPS 서명 다운로드](#)
- [Cisco IPS 서명 검색 페이지](#)
- [Cisco 보안 모니터링, 분석 및 대응 시스템](#)
- [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.