Cisco Unified Communications Manager DoS(Denial of Service) 취약성 식별 및 완화

Cisco Unified Communications Manager DoS(Denial of Service) 취약성 식별 및 완화

자문 ID: cisco-amb-20071017-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20071017-cucm

개정 1.2

2007년 10월 17일 16:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응
디바이스별 완화 및 식별
추가 정보
개정 이력
Cisco 보안 절차
관련 정보

Cisco의 대응

이 Applied Mitigation Bulletin은 PSIRT Security Advisory *Cisco Unified Communications Manager Denial of Service Vulnerabilities*에 대한 설명서이며, 관리자가 Cisco 네트워크 디바이스에 구축할 수 있는 식별 및 완화 기술을 제공합니다.

취약성 특성

CUCM(Cisco Unified Communications Manager)의 특정 릴리스에는 이전의 Cisco Unified CallManager와 같은 여러 취약점이 있습니다. 이러한 취약성은 다음 하위 섹션에 요약되어 있습니다.

SIP(Session Initiation Protocol) INVITE UDP Denial of Service: 이 취약성은 인증 없이 사용자 상호작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 DoS(서비스 거부) 조건이 발생할 수 있습니다. 이 취약성을 악용하려는 시도가 반복되면 DoS 상태가 지속될 수 있습니다. 익스플로잇을 위한 공격 벡터는 UDP 포트 5060을 사용하는 SIP 패킷을 통해 이루어집니다. 공격자는 스푸핑 공격을 통해 이 취약성을 악용할 수 있습니다. 이 취약성에는 CVE 이름 CVE-2007-5537이 할당되었습니다.

TFTP(Centralized Trivial File Transfer Protocol) File Locator Service Overflow: 이 취약성은 인증

없이 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 허용되어 DoS(서비스 거부) 조건이 발생할 수 있습니다. 이 취약성을 악용하려는 시도가 반복되면 DoS 상태가 지속될 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 6970을 사용하는 HTTP 패킷을 통해 이루어집니다. 이 취약성에는 CVE 이름 CVE-2007-5538이 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-20071017-cucm

완화 기법 개요

Cisco 디바이스는 SIP INVITE UDP Denial of Service 및 Centralized TFTP File Locator Service 오버플로 취약성에 대한 몇 가지 대응책을 제공합니다. 관리자는 이러한 보호 방법을 인프라 디바이스 및 네트워크를 이동하는 트래픽에 대한 일반적인 보안 모범 사례로 고려하는 것이 좋습니다.

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 이 문서에 설명된 취약성을 악용하려는 패킷의 소스 IP 주소를 확인하고 필터링합니다.

Cisco IOS Software에서 유니캐스트 RPF의 올바른 구축 및 컨피그레이션은 스푸핑된 소스 IP 주소의 패킷을 사용하는 공격에 대해 가장 효과적인 보호 방법을 제공합니다. 유니캐스트 RPF는 가능한 한 모든 트래픽 소스에 가깝게 구축해야 합니다.

IPSG의 올바른 구축 및 컨피그레이션은 스푸핑된 소스 MAC 주소를 사용하여 공격에 대한 가장 효과적인 보호 수단을 제공합니다.

다음을 사용하여 Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 FWSM(Firewall Services Module)에서도 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다.

- tACL
- 유니캐스트 RPF

이러한 보호 메커니즘은 이 문서에 설명된 취약성을 악용하려는 패킷의 소스 IP 주소를 확인하고 필터링합니다.

Cisco ASA, PIX 및 FWSM에서 유니캐스트 RPF의 적절한 구축 및 컨피그레이션은 스푸핑된 소스 IP 주소와 함께 패킷을 사용하는 공격에 대해 가장 효과적인 보호 수단을 제공합니다. 유니캐스트 RPF는 가능한 한 모든 트래픽 소스에 가깝게 구축해야 합니다.

Cisco IOS NetFlow는 플로우 레코드를 사용하여 이러한 익스플로잇 시도에 대한 가시성을 제공할 수 있습니다.

Cisco IOS Software, Cisco ASA, Cisco PIX 보안 어플라이언스 및 FWSM 방화벽은 syslog 메시지 및 **show** 명령의 출력에 표시되는 카운터 값을 통해 가시성을 제공할 수 있습니다.

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

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

위험 관리

조직은 표준 위험 평가 및 완화 프로세스에 따라 이러한 취약성의 잠재적인 영향을 파악해야 합니다. 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 정보 보안 관련 계약의 위험 분류 및 프로토타이핑은 조직이 반복 가능한 보안 평가 및 대응 프로세스를 개발하는 데 도움이 될 수 있습니다.

디바이스별 완화 및 식별

주의: 어떤 완화 기술이든 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, PIX 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 보호하기 위해 관리자는 트랜짓 액세스 제어 목록(tACL)을 구축하여 정책 시행을 수행해야 합니다. 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 정책은 영향을 받는 디바이스에 전송된 UDP 포트 5060의 무단 SIP 패킷 및 TCP 포트 6970의 HTTP 패킷을 거부합니다. 다음 예에서 192.168.1.0/24은 영향을 받는 디바이스에서 사용하는 네트워크 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 정보는 Transit Access Control List: Filtering at Your Edge에서 확인할 수 있습니다.

```
! !--- Include any explicit permit statements for trusted sources !--- that require access on the vulnerable ports ! access-list 150 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970 ! !--- The following vulnerability-specific access control entries !--- (ACEs) can aid in identification of attacks ! access-list 150 deny udp any 192.168.1.0 0.0.0.255 eq 5060 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 ! !--- Permit/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 unreachable을 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.

유니캐스트 역방향 경로 전달

SIP INVITE UDP Denial of Service 취약성은 스푸핑된 IP 패킷에 의해 악용될 수 있습니다. 유니캐스트 RPF(Unicast Reverse Path Forwarding)의 적절한 구축 및 컨피그레이션은 SIP INVITE UDP 서비스 거부 취약성과 관련된 스푸핑을 위한 보호 메커니즘을 제공할 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 100% 스푸핑 보호를 제공하기 위해 유니캐스트 RPF에 의존해서는 안 됩니다. 이 기능을 구축하는 동안 네트워크를 전송하는 합법적인 트래픽을 삭제할 수 있으므로 관리자는 적절한 유니캐스트 RPF 모드(느슨하거나 엄격함)가 구성되었는지 확인해야 합니다. 엔터프라이즈 환경에서는 인터넷 에지와 사용자 지원 레이어 3 인터페이스의 내부 액세스 레이어에서 유니캐스트 RPF가 활성화될 수 있습니다.

추가 정보는 Unicast Reverse Path Forwarding Loose Mode Feature Guide에서 확인할 수 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 스푸핑하려고 시도하는 공격자의 공격을 방지할 수 있습니다. 엄격한 모드 유니캐스트 RPF와 결합된 IPSG의 적절한 구축 및 구성은 SIP INVITE UDP 서비스 거부 취약성을 완화하는 데 도움이 되는 가장 효과적인 스푸핑 보호 방법을 제공할 수 있습니다.

IPSG의 구축 및 컨피그레이션에 대한 자세한 내용은 DHCP 기능 및 IP Source Guard 구성에서 확인할 수 있습니다.

식별: 통과 액세스 제어 목록

관리자가 인터페이스에 tACL을 적용한 후 **show ip access-lists 명령**은 필터링된 UDP 포트 5060의

SIP 패킷 및 TCP 포트 6970의 HTTP 패킷 수를 식별합니다. 관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인해야 합니다. **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 udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970
    30 deny udp any 192.168.1.0 0.0.0.255 eq 5060 (12 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 (26 matches)
    50 deny ip any any
router#
```

앞의 예에서 액세스 목록 150은 ACE 시퀀스 ID 30에 대해 UDP 포트 5060에서 12개의 SIP 패킷을 삭제했고, ACE 시퀀스 ID**40에 대해 TCP** 포트 6970**에서 26개**의 **HTTP 패킷을 삭제했습니다.**

ID: 액세스 목록 로깅

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

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

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. **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 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 ip interface, **show cef drop**, **show cef interface** *type slot/port* **internal** 및 **show ip traffic 명령을** 사용하여 유니캐스트 RPF가 삭제한 패킷의 수를 식별할 수 있습니다.

참고: show **명령**은 | **regexp** *시작* 및 **show** *명령* | **include** *regexp* command modifiers는 관리자가 원하는 정보를 보기 위해 구문 분석해야 하는 출력의 양을 최소화하기 위해 다음 예에서 사용됩니다. 명령 수정자에 대한 자세한 내용은 Cisco IOS Configuration Fundamentals Command Reference(Cisco IOS 컨피그레이션 기본 사항 명령 참조)의 "show command" 섹션에서 확인할 수 있습니다.

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

```
router#show ip interface GigabitEthernet 0/0 | begin verify
    !--- CLI Output Truncated
   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
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route    No_adj
RP             0           0           0           3         0
router#


router#show cef interface GigabitEthernet 0/0 internal | include drop
      --      CLI Output Truncated       --
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow self-ping
router#


router#show ip traffic

IP statistics:
  Rcvd:  68051015 total, 2397325 local destination
         43999 format errors, 0 checksum errors, 33 bad hop count
         2 unknown protocol, 929 not a gateway
         21 security failures, 190123 bad options, 542768 with options
  Opts:  352227 end, 452 nop, 36 basic security, 1 loose source route
         45 timestamp, 59 extended security, 41 record route
         53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
         361634 other
  Frags: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 64666 received, 0 sent
  Mcast: 1589885 received, 2405454 sent
  Sent:  3001564 generated, 65359134 forwarded

  Drop:  4256 encapsulation failed, 0 unresolved, 0 no adjacency
         18 no route, 18 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
    !--- CLI Output Truncated router#
```

앞의 예에서는 Cisco Express Forwarding Forwarding Information Base 내에서 IP 패킷의 소스 주소를 확인할 수 없어 유니캐스트 RPF가 구성된 모든 인터페이스에서 유니캐스트 RPF가 전체적으로 수신한 **18개**의 IP 패킷을 삭제했습니다.

Cisco IOS NetFlow

식별: NetFlow 레코드를 사용한 트래픽 흐름 식별

관리자는 Cisco IOS 라우터 및 스위치에서 Cisco IOS NetFlow를 구성하여 이 문서에 설명된 취약성을 악용하려는 시도일 수 있는 트래픽 흐름을 식별할 수 있도록 지원할 수 있습니다. 관리자는 플로우를 조사하여 이러한 취약성을 악용하려는 시도인지 또는 올바른 트래픽 플로우인지 확인해야 합니다.

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

```
IP packet size distribution (1103375 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .004 .434 .081 .017 .011 .033 .001 .010 .001 .000 .009 .000 .001 .001 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .002 .380 .002 .004 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  12 active, 65524 inactive, 54766 added
  3098504 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
  IP Sub Flow Cache, 402120 bytes
  24 active, 16360 inactive, 109532 added, 54766 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         869      0.0        38    41      0.1      20.6      43.2
TCP-FTP             31      0.0        16    59      0.0       6.7      28.0
TCP-WWW           2996      0.0        12   231      0.1       8.2      11.4
TCP-other        24997      0.0        38   288      3.3      25.5      21.1
UDP-DNS            361      0.0         2    49      0.0       0.9      60.4
UDP-NTP          13982      0.0         1    76      0.0       0.8      60.5
UDP-other        10136      0.0         3   159      0.1      25.3      48.6
ICMP               556      0.0         7    68      0.0      51.4      39.6
Total:           53928      0.1        20   270      3.7      18.1      36.8

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64  Gi0/1         192.168.1.21    11 13C4 13C4  1458
Gi0/0         192.16820.67    Gi0/1         192.168.150.60  06 0707 0016    80
Gi0/0         192.168.208.63  Gi0/1         192.168.1.21    06 84F2 1B3A     4
Gi0/0         192.168.14.132  Gi0/1         192.168.150.60  06 1A29 90AB     2
Gi0/0         192.168.115.113 Gi0/1         192.168.128.21  06 09BD 0017     2
Gi0/0         192.168.115.113 Local         192.168.128.20  06 0981 0017    31
Gi0/0         192.168.115.113 Gi0/1         192.168.130.41  06 0B83 01BB    30
Gi0/0         192.168.226.1   Gi0/1         192.168.206.5   11 007B 007B     1
Gi0/0         192.168.226.1   Local         192.168.128.20  11 007B 007B     1
Gi0/0         192.168.226.1   Gi0/1         192.168.128.21  11 007B 007B     1
router#
```

앞의 예에서는 UDP 포트 5060의 SIP 패킷(16진수 값 13C4)과 TCP 포트 6970의 HTTP 패킷(16진수 값 1B3A)에 대한 여러 플로우가 있습니다. 이러한 흐름의 UDP 패킷은 스푸핑될 수 있으며, 이 문서에 설명된 취약성을 악용하려는 시도를 나타낼 수 있습니다. 관리자는 이러한 흐름을 UDP 포트 5060 및 TCP 포트 6970의 SIP 패킷에 대한 기본 사용률과 비교하고, 흐름이 신뢰할 수 없는 호스트 또는 네트워크에서 소싱되는지 확인하기 위해 조사해야 합니다.

UDP 포트 5060(16진수 값 13C4)에서 SIP 패킷에 대한 트래픽 흐름만 보려면, 명령 show ip cache flow | include SrcIf|_11_.*13C4는 여기에 표시된 것과 같은 관련 NetFlow 레코드를 표시합니다.

```
router#show ip cache flow | include SrcIf|_11_.*13C4
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64   Gi0/1 192.168.1.21    11 13C4 13C4  1458
router#
```

TCP 포트 6970에 대한 트래픽 흐름(16진수 값 1B3A)만 보려면 명령은 show ip cache flow를 실행합니다 | include SrcIf|_06_.*1B3A는 여기에 표시된 대로 관련 NetFlow 레코드를 표시합니다.

```
router#show ip cache flow | include SrcIf|_06_.*1B3A
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
```

```
Gi0/0          192.168.208.63   Gi0/1 192.168.1.21    06 84F2 1B3A     4
router#
```

Cisco ASA, PIX 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 보호하기 위해 관리자는 tACL을 구축하여 정책 적용을 수행해야 합니다. 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 정책은 영향을 받는 디바이스에 전송된 UDP 포트 5060의 무단 SIP 패킷 및 TCP 포트 6970의 HTTP 패킷을 거부합니다. 다음 예에서 192.168.1.0/24은 영향을 받는 디바이스에서 사용하는 네트워크 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 정보는 Transit Access Control List: Filtering at Your Edge에서 확인할 수 있습니다.

```
! !--- Include any explicit permit statements for trusted sources !--- that require
access on the vulnerable ports ! access-list Transit-ACL-Policy extended permit udp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 6970 ! !--- The
following vulnerability-specific access control entries !--- (ACEs) can aid in
identification of attacks ! access-list Transit-ACL-Policy extended deny udp any
192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy extended deny tcp
any 192.168.1.0 255.255.255.0 eq 6970 ! !--- Permit/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 Transit-ACL-Policy extended
deny ip any any ! !--- Apply tACL to interfaces in the ingress direction ! access-
group Transit-ACL-Policy in interface outside
```

완화: 유니캐스트 역방향 경로 전달을 사용한 스푸핑 보호

SIP INVITE UDP Denial of Service 취약성은 스푸핑된 IP 패킷에 의해 악용될 수 있습니다. 유니캐스트 RPF(Unicast Reverse Path Forwarding)의 적절한 구축 및 컨피그레이션은 SIP INVITE UDP 서비스 거부 취약성과 관련된 스푸핑을 위한 보호 메커니즘을 제공할 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 100% 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 명령**을 사용하여 필터링된 UDP 포트 5060의 SIP 패킷 및 TCP 포트 6970의 HTTP 패킷 수를 식별할 수 있습니다. 관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인해야 합니다. show access-**list Transit-ACL-Policy**의 출력 **예는 다음과** 같습니다.

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1
192.168.1.0 255.255.255.0 eq sip
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 6970
access-list Transit-ACL-Policy line 3 extended deny udp any 192.168.1.0 255.255.255.0
eq sip (hitcnt=4378)
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255.255.0
eq 6970
access-list Transit-ACL-Policy line 5 extended deny ip any any
firewall#
```

앞의 예에서 액세스 목록 *Transit-ACL-Policy*는 신뢰할 수 없는 호스트 또는 네트워크로부터 수신한 UDP 포트 **5060**에서 **4378**개의 SIP 패킷을 삭제했습니다. 또한 syslog 메시지 *106023*은 소스 및 목적지 IP 주소, 소스 및 목적지 포트 번호, 거부된 패킷에 대한 IP 프로토콜을 포함하는 중요한 정보를 제공할 수 있습니다.

ID: 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 Security Appliance System Log Message - 106023에서 확인할 수 있습니다.

Cisco ASA 5500 Series Adaptive Security Appliance 또는 Cisco PIX 500 Series Security Appliance에 대한 syslog 구성 정보는 Cisco Security Appliance에서 로깅 구성을 참조하십시오. Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 Cisco FWSM의 모니터링 및 로깅 구성에 나와 있습니다.

다음 예에서는 **show logging | grep** *regex* 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 이 문서에 설명된 취약성을 악용하려는 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 자세한 내용은 Using the Command Line Interface를 참조하십시오.

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-4-106023: Deny udp src outside:192.168.2.18/5210 dst
   inside:192.168.1.191/5060 by access-group "Transit-ACL-Policy"
Sep 20 2007 10:07:01: %ASA-4-106023: Deny tcp src outside:192.168.3.200/3521 dst
   inside:192.168.1.33/6970 by access-group "Transit-ACL-Policy"
firewall#
```

앞의 예에서 액세스 목록 *Transit-ACL-Policy*는 신뢰할 수 없는 호스트 또는 네트워크로부터 수신한 UDP 포트 **5060**에서 **4378**개의 SIP 패킷을 삭제했습니다. 또한 syslog 메시지 *106023*은 소스 및 목적지 IP 주소, 소스 및 목적지 포트 번호, 거부된 패킷에 대한 IP 프로토콜을 포함하는 중요한 정보를 제공할 수 있습니다.

ASA 및 PIX 보안 어플라이언스의 syslog 메시지에 대한 추가 정보는 Cisco Security Appliance System Log Messages에서 확인할 수 있습니다. FWSM용 syslog 메시지에 대한 추가 정보는 Catalyst 6500 Series Switch 및 Cisco 7600 Series Router Firewall Services Module 로깅 컨피그레

이션 및 시스템 로그 메시지에서 확인할 수 있습니다.

식별: 유니캐스트 역방향 경로 전달을 사용하는 스푸핑 보호

유니캐스트 RPF에서 *거부된 패킷*에 대해 방화벽 syslog 메시지 106021이 생성됩니다. 이 syslog 메시지에 대한 추가 정보는 Cisco Security Appliance System Log Message - 106021에서 제공됩니다.

Cisco ASA 5500 Series Adaptive Security Appliance 또는 Cisco PIX 500 Series Security Appliance에 대한 syslog 구성 정보는 Cisco Security Appliance에서 로깅 구성을 참조하십시오. Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 Cisco FWSM의 모니터링 및 로깅 구성에 나와 있습니다.

다음 예에서는 **show logging | grep** *regex* 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 이 문서에 설명된 취약성을 악용하려는 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 자세한 내용은 Using the Command Line Interface를 참조하십시오.

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny TCP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
firewall#
```

다음 **예와** 같이 show asp drop 명령은 유니캐스트 RPF에서 삭제한 패킷의 수를 식별할 수도 있습니다.

```
firewall#show asp drop

Frame drop:
  Reverse-path verify failed                              11
  Flow is denied by configured rule                      855
  Expired flow                                             1
  Interface is down                                        2

Flow drop:

firewall#
```

앞의 예에서 Unicast RPF는 Unicast RPF가 구성된 인터페이스에서 수신된 **11**개의 **IP** 패킷을 삭제했습니다.

유니캐스트 RPF의 컨피그레이션 및 사용에 대한 자세한 내용은 Cisco Security Appliance Command Reference for **show asp drop을 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 취약성을 악용하려는 시도를 방지할 수 있습니다. 이러한 취약성은 다음 서명에 의해 탐지될 수 있습니다.

- 5912/0 - CUCM SIP INVITE UDP Denial of Service
- 5910/0 - CUCM 중앙 TFTP 파일 로케이터 서비스 버퍼 오버플로

5912/0 - CUCM SIP INVITE UDP Denial of Service.

Cisco IPS 버전 6.x 또는 5.x를 실행하는 센서의 시그니처 업데이트 S307부터 이 문서에 설명된 취약성은 시그니처 6912/0(시그니처 이름: CUCM Centralized TFTP File Locator Service Buffer Overflow)으로 탐지할 수 있습니다. Signature 5912/0은 기본적으로 활성화되어 *Medium* 심각도 이벤트를 트리거하며 SFR(Signature Fidelity Rating)이 80이고 기본 이벤트 작업인 Produce Alert로 **구성됩니다**. 시그니처 5912/0은 UDP 포트 5060을 사용하여 전송된 여러 패킷이 감지될 때 발생합니다. 이 서명의 실행은 이 문서에 설명된 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

5910/0 - CUCM 중앙 TFTP 파일 로케이터 서비스 버퍼 오버플로입니다.

Cisco IPS 버전 6.x 또는 5.x를 실행하는 센서의 시그니처 업데이트 S307부터 이 문서에 설명된 취약성은 시그니처 5910/0(시그니처 이름: CUCM Centralized TFTP File Locator Service Buffer Overflow)으로 탐지할 수 있습니다. 서명 5910/0은 기본적으로 활성화되어 *중간* 심각도 이벤트를 트리거하고 SFR이 75이며 기본 이벤트 작업인 **Produce Alert로 구성됩니다**. 시그니처 5910/0은 TCP 포트 6970을 사용하여 전송된 여러 패킷이 탐지될 때 발생합니다. 이 서명의 실행은 이 문서에 설명된 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.

이 취약성을 악용하려면 3방향 TCP 핸드셰이크를 설정해야 합니다. 그러면 스푸핑된 IP 주소를 사용하는 성공적인 공격과 시그니처 5910/0에 대한 오탐 이벤트의 가능성이 줄어듭니다.

UDP 기반 익스플로잇은 쉽게 스푸핑될 수 있으므로, 스푸핑된 주소를 포함하는 공격은 구성된 이벤트 작업이 신뢰할 수 있는 소스의 트래픽을 실수로 거부하게 할 수 있습니다. ACL 또는 shun 명령을 통해 차단을 수행하는 이벤트 작업은 일반적으로 프로미스큐어스 모드로 구축된 센서에 구성됩니다.

Cisco IPS 센서는 이벤트 동작의 사용과 결합된 인라인 보호 모드에서 구축될 때 가장 효과적입니다. 인라인 보호 모드로 구축된 Automatic Threat Prevention for Cisco IPS 6.x 센서는 이러한 취약점을 악용하려는 공격에 대한 위협 방지 기능을 제공합니다. 위협 방지는 RiskRatingValue가 90보다 큰 트리거된 시그니처에 대해 **Deny Connection Inline(연결 인라인 거부)** 및 **Produce Alert(경고 생성)**의 이벤트 작업을 수행하는 기본 재정의를 통해 *이루어집니다*. 위험 등급 및 그 가치 계산에 대한 자세한 내용은 Cisco IPS Risk Rating Described(설명된 IPS 위험 등급)에서 확인할 수 있습니다.

인라인 보호 모드로 구축된 Cisco IPS 5.x 센서에는 서명 단위로 이벤트 작업이 구성되어 있어야 합니다. 또는 관리자는 트리거되고 고위험 위협으로 계산된 모든 서명에 대해 이벤트 작업을 수행할 수 있는 재정의를 구성할 수 있습니다. 인라인 보호 **모드**에서 **배포된 센서**에 대해 Deny **Connection Inline** and **Produce Alert** 이벤트 작업을 사용하면 가장 효과적인 익스플로잇 방지 기능이 제공됩니다.

식별: IPS 서명 이벤트

5912/0 - CUCM SIP INVITE UDP Denial of Service.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278931859 severity=medium vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:14:21 2007/10/17 12:14:21 CDT
  signature: description=CUCM SIP INVITE UDP Denial of Service id=5912 version=S307
    subsigId: 0
    sigDetails: CUCM SIP INVITE UDP Denial of Service
    marsCategory: DoS/Network/UDP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.64
      port: 5060
    target:
      addr: locality=OUT 192.168.132.44
      port: 5060
      os: idSource=learned relevance=relevant type=linux
   triggerPacket:
 !--- Packet details removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 60 threatRatingValue: 60 interface: ge0_0 protocol: udp
```

5910/0 - CUCM 중앙 TFTP 파일 로케이터 서비스 버퍼 오버플로입니다.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278930978 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:00:57 2007/10/17 12:00:57 CDT
  signature: description=CUCM Centralized TFTP File Locator Service Buffer Overflow
id=5910 version=S307
    subsigId: 0
    sigDetails: Buffer overflow in TFTP over HTTP
    marsCategory: Penetrate/BufferOverflow/Web
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
      port: 32806
    target:
      addr: locality=OUT 192.168.132.44
      port: 6970
      os: idSource=learned relevance=relevant type=linux
    context:
      fromAttacker:
!--- Packet Details Removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium watchlist=25 81 threatRatingValue: 81 interface: ge0_0
protocol: tcp
```

Cisco 보안 모니터링, 분석 및 대응 시스템

식별: Cisco 보안 모니터링, 분석 및 응답 시스템 쿼리 유형 및 키워드

Cisco Security MARS(Monitoring, Analysis, and Response System) 어플라이언스는 쿼리 유형 및

키워드를 사용하여 CUCM 서비스 거부 취약성에 대한 이벤트에 쿼리할 수 있습니다. SIP INVITE UDP 서비스 거부 취약성을 탐지할 수 있는 IPS signature **5912/0의 경우 NR-5912/0**의 키워드를 사용하고, 중앙 집중식 TFTP 파일 로케이터 서비스 오버플로 취약성을 탐지할 수 있는 IPS signature **5910/0**의 경우 **NR-5910/0**의 키워드를 사용하며,**Cisco Security MARS Appliance의 모든 Matching Event Raw Messages의 쿼리 유형은 IPS signature 5912/0 또는 5910/0에 의해 생성된 이벤트를 나열하는 보고서를 제공합니다.**

다음 스크린샷은 IPS 서명 5912/0(서명 이름: CUCM SIP INVITE UDP Denial of Service) 또는 IPS 서명 5910/0(서명 이름: CUCM Centralized TFTP File Locator Service Buffer Overflow)에 의해 생성된 이벤트를 쿼리하는 데 사용되는 값을 보여줍니다.

다음 스크린샷은 Cisco Security MARS 어플라이언스에서 쿼리 유형 및 키워드 regex 쿼리를 사용하여 생성한 **NR-5912/0 또는 NR-5910/0**에 대한 쿼리 결과를 보여줍니다.

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

개정 이력

개정 1.2	2007년 10월 22일	할당된 CVE 이름 포함
개정 1.1	2007년 10월 17일	IPS 시그니처 팩 S307 정보 포함
개정 1.0	2007년 10월 17일	초기 공개

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 Applied Mitigation 게시판
- 코어 보호: 인프라 보호 액세스 제어 목록
- 트랜짓 액세스 제어 목록: 에지에서 필터링
- 액세스 제어 목록 로깅 이해
- 유니캐스트 역방향 경로 전달 이해
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)
- Cisco IOS NetFlow 백서
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- 유니캐스트 역방향 경로 전달 느슨한 모드
- CVE(Common Vulnerabilities and Exposures)
- Cisco 6.x 침입 방지 시스템

- Cisco IPS 위험 등급 설명
- Cisco IPS 6.x 서명 다운로드
- 릴리스 버전별 Cisco IPS 서명(등록된 고객만 해당)
- 서명 ID별 Cisco IPS 서명(등록된 고객만 해당)
- Cisco 보안 모니터링, 분석 및 대응 시스템

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.