# 여러 Cisco Unified Communications Manager 및 프레즌스 서버 취약성 식별 및 완화

# 여러 Cisco Unified Communications Manager 및 프레즌스 서버 취약성 식별 및 완화

**자문 ID: cisco-amb-20070711-cucm**

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070711-cucm

## 개정 1.0

**2007년 7월 11일 16:00 UTC(GMT) 공개 릴리스의 경우**

---

## 목차



---

## Cisco의 대응

이 Applied Mitigation Bulletin은 *Cisco Unified Communications Manager Overflow Vulnerabilities* 및 *Cisco Unified Communications Manager*와 *Presence Server Unauthorized Access Vulnerabilities와 같은 PSIRT* 보안 권고와 함께 제공되는 문서로서 관리자가 Cisco 네트워크 디바이스에 구축할 수 있는 식별 및 완화 기술을 제공합니다.

### 취약성 특성

Cisco Unified Communications Manager 및 Cisco Unified Presence Server에는 여러 가지 취약점이 있습니다. 이러한 취약성은 다음 하위 섹션에 요약되어 있습니다.

**Certificate Trust List Provider Service Overflow:** 이 취약성은 인증 없이 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 허용되거나 DoS(서비스 거부) 조건이 발생할 수 있습니다. 공격 벡터는 CTL(Certificate Trust List) 제공자 서비스 포트로 전송되는 패킷입니다. 기본 포트는 TCP 포트 2444입니다. 관리자는 Cisco Unified Communications Manager GUI에서 **System(시스템) > Service Parameters(서비스 매개변수)**를 선택하여 CTL Provider(CTL 제공자) 서비스가 사용하는 포트를 확인할 수 있습니다. Server(서버) 드롭다운 목록에서 서버를 선택합니다. 그런 다음 Service 드롭다운 **목록**에서 **Cisco CTL Provider (Inactive) 또는 Cisco CTL Provider (Active)**를 선택합니다. 이 목록의 서비스 *이름*에 추가된

*(Inactive)* 또는 *(Active)*라는 용어는 서비스 활성화 여부를 나타냅니다. 서비스를 선택하면 Port Number(포트 번호) 매개변수가 Server and Service(서버 및 서비스) 드롭다운 목록 아래 영역에 표시됩니다. 이 매개변수의 값은 활성 상태일 때 서비스에 사용되는 포트를 나타냅니다. 게시 당시 이 취약성과 관련된 CVE ID는 없었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어 및 고정 소프트웨어에 대한 정보는 PSIRT Security Advisory(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm)에서 확인할 수 있습니다.

**Real-Time Information Server Data Collector Heap Overflow:** 이 취약성은 인증 없이 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 허용되거나 DoS(서비스 거부) 조건이 발생할 수 있습니다. 공격 벡터는 RIS(Real-Time Information Server) 데이터 수집기 포트로 전송된 패킷입니다. 기본 포트는 TCP 포트 2556입니다. 관리자는 Cisco Unified Communications Manager GUI에서 **System(시스템) > Service Parameters(서비스 매개변수)**를 선택하여 RIS Data Collector 서비스에서 사용하는 포트를 확인할 수 있습니다. Server(서버) 드롭다운 목록에서 서버를 선택합니다. 그런 다음 Service 드롭다운 **목록**에서 **Cisco RIS Data Collector (Inactive)** 또는 **Cisco RIS Data Collector (Active)**를 선택합니다. 이 목록의 서비스 *이름*에 추가된 *(Inactive)* 또는 *(Active)*라는 용어는 서비스 활성화 여부를 나타냅니다. 서비스를 선택하면 RIS Cluster TCP Port(RIS 클러스터 TCP 포트) 매개변수가 Clusterwide Parameters(클러스터 수준 매개변수) 영역에 표시됩니다. 이 매개변수의 값은 활성 상태일 때 서비스에 사용되는 포트를 나타냅니다. 게시 당시 이 취약성과 관련된 CVE ID는 없었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어 및 고정 소프트웨어에 대한 정보는 PSIRT Security Advisory(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm)에서 확인할 수 있습니다.

**권한이 없는 관리자는 Cisco Unified Communications Manager/Cisco Unified Presence Server System Services를 활성화/종료할** 수 있습니다**:** 이 취약성은 인증 없이 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 무단 사용을 통해 Cisco Unified Communications Manager/Cisco Unified Presence Server 관리자는 클러스터 환경에서 시스템 서비스를 활성화 또는 종료할 수 있습니다. 이로 인해 중요한 음성 서비스가 중단되거나 중지될 수 있습니다. 공격 벡터는 TCP 포트 8443 패킷을 사용하는 SSL 프로토콜입니다. 영향을 받는 소프트웨어에서 사용하는 포트에 대한 자세한 내용은 Cisco CallManager TCP 및 UDP 포트 사용을 참조하십시오. 게시 당시 이 취약성과 관련된 CVE ID는 없었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어 및 고정 소프트웨어에 대한 정보는 PSIRT Security Advisory(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip)에서 확인할 수 있습니다.

**권한이 없는 관리자는 Cisco Unified Communications Manager/Cisco Unified Presence Server SNMP 설정을 볼 수 있습니다.** 이 취약성은 인증 없이 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 무단 관리자가 Cisco Unified Communications Manager/Cisco Unified Presence Server 클러스터 노드의 관리 인터페이스에서 SNMP 설정 보기를 탐색할 수 있습니다. 공격 벡터는 TCP 포트 8443 패킷을 사용하는 SSL 프로토콜입니다. 영향을 받는 소프트웨어에서 사용하는 포트에 대한 자세한 내용은 Cisco CallManager TCP 및 UDP 포트 사용을 참조하십시오. 게시 당시 이 취약성과 관련된 CVE ID는 없었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어 및 고정 소프트웨어에 대한 정보는 PSIRT Security Advisory(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20070711-voip)에서 확인할 수 있습니다.

### 완화 기법 개요

Cisco 디바이스는 이 문서에 설명된 취약성에 대한 몇 가지 대응책을 제공합니다. 관리자는 이러한 보호 방법 중 상당수를 인프라 디바이스 및 네트워크를 이동하는 트래픽에 대한 일반적인 보안 모범 사례로 고려하는 것이 좋습니다.

Cisco IOS Software는 tACL(transit access control list)을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다.

Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터를 위한 FWSM(Firewall Services Module)에서도 tACL(transit access control list)을 사용하여 효과적인 익스플로잇 방지 기능을 제공할 수 있습니다.

이러한 보호 메커니즘은 이 문서에 설명된 취약성을 악용하려는 패킷을 필터링 및 삭제합니다.

Cisco IOS NetFlow는 플로우 레코드를 사용하여 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.

### 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 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 인

그레스 액세스 포인트에서 네트워크에 들어가도록 명시적으로 허용하거나 기존 보안 정책 및 컨피그레이션에 따라 인증 받은 트래픽이 네트워크를 통과하도록 허용하여 tACL을 구성할 수 있습니다.

tACL 정책은 TCP 포트 2444의 CTL 제공자 서비스, TCP 포트 2556의 RIS 데이터 수집기 및 영향을 받는 장치로 전송되는 TCP 포트 8443의 Cisco Unified Communications Manager/Cisco Unified Presence Server System Services에 대해 무단 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 port(s) ! access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2444 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2556 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 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 192.168.1.0 0.0.0.255 eq 2444 access-list 150 deny tcp any 192.168.1.0
0.0.0.255 eq 2556 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 ! !--
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 interface(s) 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. 이렇게 하면 디바이스에서 이러한 ICMP 도달 불가 메시지를 생성해야 하므로 CPU 사용률이 증가하는 원하지 않는 영향이 발생할 수 있습니다. Cisco IOS Software에서 ICMP 연결 불가능 생성은 기본적으로 500밀리초마다 하나의 패킷으로 제한됩니다. ICMP 연결 불가능 메시지 생성은 **no icmp unreachable** interface configuration 명령을 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.

### 식별: 통과 액세스 제어 목록

관리자가 인터페이스에 tACL을 적용한 후 **show ip access-lists 명령**은 필터링된 TCP 포트 2444의 CTL 제공자 서비스 패킷 수, TCP 포트 2556의 RIS 데이터 수집기 패킷 수 및 TCP 포트 8443의 CUCM/CUPS 시스템 서비스 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 tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444 (2 matches)
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556 (3 matches)
    30 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443 (3 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 2444 (3 matches)
    50 deny tcp any 192.168.1.0 0.0.0.255 eq 2556 (4 matches)
    60 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 (5 matches)
    70 deny ip any any
router#
```

앞의 예에서 액세스 목록 150은 ACE 시퀀스 ID 40의 **TCP 포트 2444에서 3**개, ACE 시퀀스 ID 50의 **TCP 포트 2556에서 4개**, ACE 시퀀스 ID 60의 **TCP 포트 8443에서 5개**의 패킷을 삭제했습니다.

### ID: 액세스 목록 로깅

log **또는** **log-input** ACL 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 영향은 두 가지 요인, 즉 로그 지원 ACE와 일치하는 패킷의 결과로 프로세스 스위칭과 로그 생성 및 전송에 의해 결정됩니다.

ACL 로깅의 CPU 영향은 Catalyst 6500 Series 스위치와 Cisco 7600 Series 라우터(Supervisor 720 및 Supervisor 32 포함)의 하드웨어에서 최적화된 ACL 로깅을 사용하여 해결할 수 있습니다. ip **access-list logging interval** *in-ms 명령은* ACL 로깅으로 인한 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 http://www.cisco.com/web/about/security/intelligence/acl-logging.html의 Applied Intelligence 백서를 참조하십시오.

## 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 잠재적인 시도가 될 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 (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 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    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
```

```
TCP-other      47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.201 Gi0/1         192.168.1.102   06 0984 098C     1
Gi0/0         192.168.100.5   Gi0/1         192.168.1.158   06 0911 09FC     3
Gi0/0         192.168.105.60  Gi0/1         192.89.1.226    06 0016 12CA     1
Gi0/0         192.168.105.97  Gi0/1         192.168.1.28    06 0B3E 098C     5
Gi0/0         192.168.105.197 Gi0/1         192.168.1.248   06 0B3E 20FB     7
Gi0/0         192.168.1.17    Gi0/1         192.168.1.97    11 0B89 00A1     1
Gi0/0         192.168.105.7   Gi0/1         192.168.1.8     06 0B3E 20FB     4
Gi0/1         10.88.226.1     Gi0/0         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.1.239   06 0E8A 09FC     1
Gi0/1         10.89.16.226    Gi0/0         192.168.150.60  06 12CA 0901     1
router#
```

앞의 예에서는 **TCP 포트 2444(16진수 값 098C)**의 CTL 제공자 서비스, **TCP 포트 2556(16진수 값 09FC)의** RIS Data Collector 및 **TCP 포트 8443(16진수 값 20FB)의** Cisco Unified Communications Manager/Cisco Unified Presence Server System Service에 대한 몇 가지 흐름이 있습니다. 관리자는 이러한 플로우를 TCP 포트 2444, 2556, 8443에서 전송된 트래픽의 기준 사용률과 비교하고, 플로우가 신뢰할 수 없는 호스트 또는 네트워크에서 소싱되는지를 조사해야 합니다.

TCP 포트 2444의 패킷(16진수 값 098C), TCP 포트 2556의 패킷(16진수 값 09FC) 또는 TCP 포트 8443의 패킷(16진수 값 20FB)에 대한 트래픽 흐름만 보려면 명령에서 **show ip cache flow를 실행합니다 | include SrcIf|_06_.*(098C|09FC|20FB)는** 다음과 같이 관련 NetFlow 레코드를 표시합니다.

```
router#show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.110  Gi0/1         192.168.1.163   06 0E2A 098C     6
Gi0/0         192.168.105.230  Gi0/1         192.168.1.20    06 0C09 098C     1
Gi0/0         192.168.101.131  Gi0/1         192.168.1.245   06 0B66 20FB    18
Gi0/0         192.168.100.7    Gi0/1         192.168.1.162   06 0D14 09FC     1
Gi0/0         192.168.100.86   Gi0/1         192.168.1.27    06 0B7B 09FC     2
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 TCP 포트 2444의 무단 CTL 제공자 서비스 패킷, TCP 포트 2556의 RIS 데이터 수집기 패킷 및 영향을 받는 장치로 전송되는 TCP 포트 8443의 Cisco Unified Communications Manager/Cisco Unified Presence Server 시스템 서비스 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 port(s) ! access-list Transit-ACL-Policy extended permit tcp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2556 access-list
Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq 8443 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
can aid in identification of attacks ! access-list Transit-ACL-Policy extended deny
tcp any 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy extended
deny tcp any 192.168.1.0 255.255.255.0 eq 2556 access-list Transit-ACL-Policy
extended deny tcp any 192.168.1.0 255.255.255.0 eq 8443 ! !-- 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 interface(s) in the ingress
direction ! access-group Transit-ACL-Policy in interface outside !
```

**식별: 통과 액세스 제어 목록**

인터페이스에 tACL이 적용된 후 관리자는 **show access-list 명령**을 사용하여 필터링된 TCP 포트 2444의 CTL Provider 서비스 패킷 수, TCP 포트 2556의 RIS Data Collector 패킷 수 및 TCP 포트 8443의 Cisco Unified Communications Manager/Cisco Unified Presence Server System Service 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; 7 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2444 (hitcnt=2) 0xaca1615c
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2556 (hitcnt=4) 0x991fbe7d
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 8443 (hitcnt=3) 0xd2687825
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2444 (hitcnt=19) 0xc81a715d
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2556 (hitcnt=11) 0x67db99e7
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.1.0255.255.255.0
            eq 8443 (hitcnt=7) 0xb322498f
access-list Transit-ACL-Policy line 7 extended deny ip any any(hitcnt=0) 0xc797eb99
firewall#
```

앞의 예에서 액세스 목록 Transit-ACL-Policy는 신뢰할 수 없는 호스트 또는 네트워크에서 수신한 **TCP 포트 2444의 경우 19개**, **TCP 포트 2556의 경우 11개**, **TCP 포트 8443의 경우 7개**의 패킷을 삭제했습니다. 또한 syslog 메시지 106023은 소스 및 목적지 IP 주소, 소스 및 목적지 포트 번호, 거부된 패킷에 대한 IP 프로토콜을 비롯한 중요한 정보를 제공할 수 있습니다.

**식별: 방화벽 액세스 목록 Syslog 메시지**

log 키워드가 106023 ACE에 의해 거부된 패킷에 대해 방화벽 syslog 메시지 **메시지**가 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** *regexp* 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 이 문서에 설명된 취약성을 악용하려는 잠재적인 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 106023
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
            inside:192.168.1.191/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 dst
            inside:192.168.1.33/2556 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
            inside:192.168.1.240/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 dst
            inside:192.168.1.115/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
            inside:192.168.1.38/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 dst
            inside:192.168.1.250/2444 by access-group "Transit-ACL-Policy"
firewall#
```

앞의 예에서 tACL Transit-ACL-Policy에 대해 로깅된 메시지에는 네트워크 인프라에 할당된 주소 블록으로 전송된 **TCP 포트 2444에** 대한 패킷, **TCP 포트 2556에** 대한 패킷 및 **TCP 포트 8443에** 대한 패킷이 표시됩니다.

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 컨피그레이션 및 시스템 로그 메시지에서 확인할 수 있습니다.

## 추가 정보



## 개정 이력

| | | |
|---|---|---|
| 개정 1.0 | 2007년 7월 11일 | 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
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)
- Cisco IOS NetFlow 백서
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- 일반적인 취약성 및 노출 목록

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.