Cisco TelePresence 제품의 여러 취약성 식별 및 완화

Cisco TelePresence 제품의 여러 취약성 식별 및 완화

자문 ID: cisco-amb-20110223-telepresence

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence

개정 1.1

2011년 2월 23일 16:00 UTC (GMT)

목차

Cisco의 대응

이 Applied Mitigation Bulletin은 PSIRT Cisco TelePresence Bundle of Security Advisories와 함께 제공되는 문서로, 관리자가 Cisco 네트워크 디바이스에 구축할 수 있는 식별 및 완화 기술을 제공합니다. 이 AMB에서 다루는 개별 Security Advisories는 다음과 같습니다.

- Cisco TelePresence 엔드포인트 디바이스의 여러 취약점
- Cisco TelePresence Manager의 여러 취약점
- Cisco TelePresence Multipoint Switch의 여러 취약점
- Cisco TelePresence Recording Server의 여러 취약점

취약성 특성

Cisco TelePresence 제품에는 여러 취약점이 있습니다. 다음 하위 섹션에는 개별 PSIRT Security Advisories 및 각 Advisory에서 다루는 각 취약성이 요약되어 있습니다.

Cisco TelePresence 엔드포인트 장치

인증되지 않은 CGI 액세스: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스

플로잇을 위한 공격 벡터는 TCP 포트 8082를 사용하는 HTTP 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0372가 할당되었습니다.

CGI 명령 주입: 이러한 취약점은 인증을 통해 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이러한 취약점을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 443을 사용하는 잘못된 형식의 SSL(Secure Sockets Layer) 패킷을 통해 이루어집니다. 이러한 취약성에는 CVE 식별자 CVE-2011-0373, CVE-2011-0374 및 CVE-2011-0375가 할당되었습니다.

TFTP 정보 공개: 이 취약성은 인증 및 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 정보 공개가 가능하므로 공격자가 해당 디바이스에 대한 정보를 학습할 수 있습니다. 익스플로잇을 위한 공격 벡터는 UDP 포트 69를 사용하는 TFTP GET 요청 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0376이 할당되었습니다.

악성 IP 주소 주입: 이 취약점은 인증 없이, 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 DoS(서비스 거부) 상태가 지속될 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 8081 및 9501을 사용하는 잘못된 형식의 SOAP(Simple Object Access Protocol) 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0377이 할당되었습니다.

XML-RPC 명령 삽입: 이 취약성은 인증 및 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 61441 및 HTTPS를 사용하는 XML-RPC 패킷을 61445. 이 취약성에는 CVE 식별자 CVE-2011-0378이 할당되었습니다.

Cisco Discovery Protocol Remote Code Execution: 이 취약성은 인증 없이 엔드 유저 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 Cisco Discovery Protocol 패킷을 통해 이루어집니다. Cisco Discovery Protocol은 데이터 링크 레이어에서 작동하므로 공격자는 영향을 받는 디바이스에 프레임을 직접 제출할 수 있어야 합니다. 이 문서에서는 이 취약성에 대한 추가 정보를 제공하지 않습니다. 이 취약성에는 CVE 식별자 CVE-2011-0379가 할당되었습니다.

Cisco TelePresence 관리자

SOAP 인증 우회: 이 취약성은 인증 없이, 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 권한을 높일 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 8080 및 8443을 사용하는 잘못된 형식의 SOAP 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0380이 할당되었습니다.

Java RMI(Remote Method Invocation) 명령 삽입: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 1100 및 32000을 사용하여 작성된 Java RMI 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0381이 할당되었습니다.

Cisco Discovery Protocol Remote Code Execution: 이 취약성은 인증 없이 엔드 유저 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 악용할 공격 벡터는 Cisco Discovery Protocol 패킷을 통해 이루어집니다. Cisco Discovery Protocol은 데이터 링크 레이어에서 작동하므로 공격자는 영향을 받는 디바이스에 프레임을 직접 제출할 수 있어야 합니다. 이 문서에서는 이 취약성에 대한 추가 정보를 제공하지 않습니다. 이 취약성에는 CVE 식별자 CVE-2011-0379가 할당되었습니다.

Cisco TelePresence Multipoint Switch

인증되지 않은 Java 서블릿 액세스: 이러한 취약점은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이러한 취약점을 성공적으로 악용하면 권한을 높일 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 80 및 8080을 사용하여 작성된 HTTP 패킷과 TCP 포트 443을 사용하여 작성된 SSL 패킷을 통해 이루어집니다. 이러한 취약성에는 CVE 식별자 CVE-2011-0383 및 CVE-2011-0384가 할당되었습니다.

인증되지 않은 임의 파일 업로드: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 80을 사용하는 HTTP 패킷과 TCP 포트 443을 사용하는 SSL 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0385가 할당되었습니다.

Cisco Discovery Protocol Remote Code Execution: 이 취약성은 인증 없이 엔드 유저 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 악용할 공격 벡터는 Cisco Discovery Protocol 패킷을 통해 이루어집니다. Cisco Discovery Protocol은 데이터 링크 레이어에서 작동하므로 공격자는 영향을 받는 디바이스에 프레임을 직접 제출할 수 있어야 합니다. 이 문서에서는 이 취약성에 대한 추가 정보를 제공하지 않습니다. 이 취약성에는 CVE 식별자 CVE-2011-0379가 할당되었습니다.

무단 서블릿 액세스: 이 취약성은 인증을 통해 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 권한을 높일 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 80을 사용하는 HTTP 패킷과 TCP 포트 443을 사용하는 SSL 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0387이 할당되었습니다.

Java RMI Denial of Service: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 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 TCP 포트 8999를 사용하여 작성된 Java RMI 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0388이 할당되었습니다.

RTCP(Real-Time Transport Control Protocol) Denial of Service: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 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 통화 설정 중에 무작위로 선택되고 협상되는 수신 중인 RTCP 제어 포트로 전송된 악의적인 UDP 패킷을 통해 이루어집니다. 공격자는 스푸핑된 패킷을 사용하여 이 취약성을 악용할 수 있습니다. 이 취약성에는 CVE 식별자 CVE-2011-0389가 할당되었습니다.

XML-RPC Denial of Service: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 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 TCP 포트 9000을 사용하는 XML-RPC 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0390이 할당되었습니다.

Cisco TelePresence 녹음 서버

인증되지 않은 Java 서블릿 액세스: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 권한을 높일 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 80 및 8080을 사용하여 작성된 HTTP 패킷과 TCP 포트 443을 사용하여 작성된 SSL 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0383이 할당되었습니다.

CGI 명령 삽입: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 443을 사용하는 SSL 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식

별자 CVE-2011-0382가 할당되었습니다.

인증되지 않은 임의 파일 업로드: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 80을 사용하는 HTTP 패킷과 TCP 포트 443을 사용하는 SSL 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0385가 할당되었습니다.

XML-RPC 임의 파일 덮어쓰기: 이 취약성은 인증 및 최종 사용자 상호 작용 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 잘못된 형식의 XML-RPC 패킷을 통해 이루어지며, TCP 포트 12102 및 12104을 사용합니다. 이 취약성에는 CVE 식별자 CVE-2011-0386이 할당되었습니다.

Cisco Discovery Protocol Remote Code Execution: 이 취약성은 인증 없이 엔드 유저 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 가능할 수 있습니다. 익스플로잇을 위한 공격 벡터는 Cisco Discovery Protocol 패킷을 통해 이루어집니다. Cisco Discovery Protocol은 데이터 링크 레이어에서 작동하므로 공격자는 영향을 받는 디바이스에 프레임을 직접 제출할 수 있어야 합니다. 이 문서에서는 이 취약성에 대한 추가 정보를 제공하지 않습니다. 이 취약성에는 CVE 식별자 CVE-2011-0379가 할당되었습니다.

Ad-Hoc Recording Denial of Service: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 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 TCP 포트 80을 사용하는 HTTP 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0391이 할당되었습니다.

Java RMI Denial of Service: 이 취약성은 인증 없이 그리고 최종 사용자 상호 작용 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 TCP 포트 8999를 사용하여 작성된 Java RMI 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0388이 할당되었습니다.

인증되지 않은 XML-RPC 인터페이스: 이 취약성은 인증 없이, 그리고 최종 사용자 상호 작용 없이 로컬에서 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 작업을 수행할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 8080을 사용하는 XML-RPC 패킷을 통해 이루어집니다. 이 취약성에는 CVE 식별자 CVE-2011-0392가 할당되었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어, 고정된 소프트웨어에 대한 정보는 다음 링크에서 확인할 수 있는 개별 PSIRT 보안 권고에서 확인할 수 있습니다.

- Cisco TelePresence 엔드포인트 디바이스의 여러 취약점
- Cisco TelePresence Manager의 여러 취약점
- Cisco TelePresence Multipoint Switch의 여러 취약점
- Cisco TelePresence Recording Server의 여러 취약점

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
.

- iACL(Infrastructure Access Control Lists)
- 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 6500 Series 스위치와 Cisco 7600 Series 라우터용 Cisco FWSM(Firewall Services Module)에서는 다음을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수도 있습니다.

- 트랜짓 액세스 제어 목록(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.

Cisco TelePresence 환경을 보호할 때 고려해야 할 다양한 측면에 대한 자세한 내용은 Cisco TelePresence 강화 가이드를 참조하십시오.

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: 인프라 액세스 제어 목록

인프라 디바이스를 보호하고 직접 인프라 공격의 위험, 영향 및 효과를 최소화하기 위해 관리자는 인프라 장비에 전송된 트래픽의 정책 시행을 수행하기 위해 iACL(infrastructure access control list)을 구축하는 것이 좋습니다. 관리자는 기존 보안 정책 및 컨피그레이션에 따라 인프라 디바이스로 전송되는 승인된 트래픽만 명시적으로 허용하여 iACL을 구성할 수 있습니다. 인프라 디바이스를 최대한 보호하려면 구축된 iACL을 IP 주소가 구성된 모든 인터페이스의 인그레스 방향으로 적용해야 합니다. iACL 해결 방법은 공격이 신뢰할 수 있는 소스 주소에서 시작되는 경우 이러한 취약성에 대한 완벽한 보호를 제공할 수 없습니다.

iACL 정책은 영향을 받는 디바이스로 전송되는 다음 프로토콜/포트의 무단 패킷을 거부합니다.

- TCP 포트 80
- TCP 포트 443
- TCP 포트 1100
- TCP 포트 8080
- TCP 포트 8081
- TCP 포트 8082
- TCP 포트 8443
- TCP 포트 8999
- TCP 포트 9000
- TCP 포트 9501
- TCP 포트 12102
- TCP 포트 12104
- TCP 포트 32000
- TCP 포트 61441
- TCP 포트 61445
- UDP 포트 69

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. 인프라 주소 공간은 가능한 경우 사용자 및 서비스 세그먼트에 사용되는 주소 공간과 구분되어야 합니다. 이 주소 지정 방법론을 사용하면 iACL의 구축 및 구축에 도움이 됩니다.

iACL에 대한 추가 정보는 코어 보호: Infrastructure Protection Access Control Lists에 있습니다.

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 permit tcp host
```

```
192.168.100.1 192.168.60.0 0.0.0.255 eq 1100 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8080 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 8081 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8999 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 9000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 12102 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 12104 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 32000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445 permit udp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 69 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! deny tcp any
192.168.60.0 0.0.0.255 eq 80 deny tcp any 192.168.60.0 0.0.0.255 eq 443 deny tcp any
192.168.60.0 0.0.0.255 eq 1100 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 deny tcp
any 192.168.60.0 0.0.0.255 eq 8081 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 deny
tcp any 192.168.60.0 0.0.0.255 eq 8443 deny tcp any 192.168.60.0 0.0.0.255 eq 8999
deny tcp any 192.168.60.0 0.0.0.255 eq 9000 deny tcp any 192.168.60.0 0.0.0.255 eq
9501 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 deny tcp any 192.168.60.0 0.0.0.255
eq 12104 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 deny tcp any 192.168.60.0
0.0.0.255 eq 61441 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 deny udp any
192.168.60.0 0.0.0.255 eq 69 ! !-- Explicit deny ACE for traffic sent to addresses
configured within !-- the infrastructure address space ! deny ip any 192.168.60.0
0.0.0.255 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-
- with existing security policies and configurations ! !-- Apply iACL to interfaces
in the ingress direction ! interface GigabitEthernet0/0 ip access-group
Infrastructure-ACL-Policy 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 환경 설정 명령어 no ip unreachable을 사용하여 비활성화할 수 있습니다. ICMP 연결 불가능 속도 제한은 기본값에서 전역 환경 설정 명령 ip icmp rate-limit unreachable interval-in-ms를 사용하여 변경할 수 있습니다.

완화: 스푸핑 보호

유니캐스트 역방향 경로 전달

이 문서에 설명된 취약성 중 하나는 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 있습니다.

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 스푸핑하려고 시도하는 공격자의 공격을 방지할 수 있습니다. IPSG를 올바르게 구축하고 구성하면 엄격한 모드 유니캐스트 RPF와 결합하여 이 문서에 설명된 취약성에 대한 가장 효과적인 스푸핑 보호 방법을 제공합니다.

IPSG 구축 및 컨피그레이션에 대한 추가 정보는 DHCP 기능 및 IP 소스 가드 구성에 있습니다.

식별: 인프라 액세스 제어 목록

관리자가 인터페이스에 iACL을 적용한 후 show ip access-lists 명령은 iACL이 적용된 인터페이스에서 필터링된 다음 프로토콜/포트의 패킷을 식별합니다.

- TCP 포트 80
- TCP 포트 443
- TCP 포트 1100
- TCP 포트 8080
- TCP 포트 8081
- TCP 포트 8082
- TCP 포트 8443
- TCP 포트 8999
- TCP 포트 9000
- TCP 포트 9501
- TCP 포트 12102
- TCP 포트 12104
- TCP 포트 32000
- TCP 포트 61441
- TCP 포트 61445
- UDP 포트 69

관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인해야 합니다. show ip access-lists에 대한 출력의 예는 다음과 같습니다.

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1100
    40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8081
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 (1 match)
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8999
    90 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9000
    100 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501
    110 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12102
    120 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12104
    130 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 32000
    140 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441
    150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445
    160 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq tftp
    170 deny tcp any 192.168.60.0 0.0.0.255 eq www (703 matches)
```

```
    180 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (213 matches)
    190 deny tcp any 192.168.60.0 0.0.0.255 eq 1100 (95 matches)
    200 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (115 matches)
    210 deny tcp any 192.168.60.0 0.0.0.255 eq 8081 (119 matches)
    220 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 (86 matches)
    230 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (125 matches)
    240 deny tcp any 192.168.60.0 0.0.0.255 eq 8999 (63 matches)
    250 deny tcp any 192.168.60.0 0.0.0.255 eq 9000 (3 matches)
    260 deny tcp any 192.168.60.0 0.0.0.255 eq 9501 (142 matches)
    270 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 (127 matches)
    280 deny tcp any 192.168.60.0 0.0.0.255 eq 12104 (132 matches)
    290 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 (125 matches)
    300 deny tcp any 192.168.60.0 0.0.0.255 eq 61441 (110 matches)
    310 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 (114 matches)
    320 deny udp any 192.168.60.0 0.0.0.255 eq tftp (218 matches)
    330 deny ip any 192.168.60.0 0.0.0.255 (9 matches)
router#
```

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

- ACE 라인 170용 TCP 포트 80(www)의 703개 HTTP 패킷
- ACE 라인 180용 TCP 포트 443의 213개 SSL 패킷
- ACE 라인 190용 TCP 포트 1100의 95개 패킷
- ACE 라인 200용 TCP 포트 8080의 115개 패킷
- ACE 라인 210용 TCP 포트 8081의 패킷 119개
- ACE 라인 220용 TCP 포트 8082의 86개 패킷
- ACE 라인 230용 TCP 포트 8443의 125개 패킷
- ACE 라인 240용 TCP 포트 8999의 63개 패킷
- ACE 라인 250용 TCP 포트 9000의 패킷 3개
- ACE 라인 260용 TCP 포트 9501의 142개 패킷
- ACE 라인 270에 대한 TCP 포트 12102의 127개 패킷
- ACE 라인 280에 대한 TCP 포트 12104의 132개 패킷
- ACE 라인 290에 대한 TCP 포트 32000의 125개 패킷
- ACE 라인 300에 대한 TCP 포트 61441의 110개 패킷
- ACE 라인 310에 대한 TCP 포트 61445의 114개 패킷
- ACE 라인 320용 UDP 포트 69의 218개 TFTP 패킷

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 백서에서는 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 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 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 명령**이 **show ip cef switching statistics 기능으로 대체되었습니다**.

참고: show **명령**은 **| begin** regex and **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 예시**에서 Unicast RPF는 **Cisco** Express Forwarding의 Forwarding Information Base 내에서 IP 패킷의 소스 주소를 확인할 수 없기 때문에 유니캐스트 RPF가 구성된 모든 인터페이스에서 전역적**으로 수신한 18개 IP 패킷**을 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 (1779 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .323 .676 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

IP Flow Switching Cache, 278544 bytes
  183 active, 3913 inactive, 364 added
  4883 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 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-WWW             16      0.0         7    40      0.0       0.0      15.7
TCP-other          126      0.0         3    40      0.1       0.0      15.4
UDP-TFTP             7      0.0         6    28      0.0       0.0      15.6
UDP-other           32      0.0         6    28      0.0       0.0      15.4
Total:             181      0.0         4    36      0.1       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.21.36   Et0/1         192.168.60.17   11 CD3E 0045     1
Et0/0         192.168.100.31  Et0/1         192.168.60.210  06 8F8C 044C     6
Et0/0         192.168.100.14  Et0/1         192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1         192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1         192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.159.166 Et0/1         192.168.90.53   11 62E2 B413    10
Et0/0         192.168.100.164 Et0/1         192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1         192.168.60.30   06 E440 1F92     6
Et0/0         192.168.12.204  Et0/1         192.168.162.10  11 39D3 9273    10
Et0/0         192.168.100.211 Et0/1         192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1         192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1         192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2327     4
```

```
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2328     4
Et0/0         192.168.194.210 Et0/1         192.168.4.64    11 85DE BE0C     5
Et0/0         192.168.100.171 Et0/1         192.168.60.215  06 84F3 1F91     1
Et0/0         192.168.100.121 Et0/1         192.168.60.165  06 15A0 2F48     8
Et0/0         192.168.100.97  Et0/1         192.168.60.22   06 0951 2327     1
Et0/0         192.168.100.221 Et0/1         192.168.60.170  06 DBCF 0050    10
Et0/0         192.168.6.90    Et0/1         192.168.243.120 06 14E7 773D    10
Et0/0         192.168.100.174 Et0/1         192.168.60.239  06 0414 1F91     5
Et0/0         192.168.100.51  Et0/1         192.168.60.109  06 EF9D 251D     2
Et0/0         192.168.78.53   Et0/1         192.168.60.37   11 07A2 0045     2
Et0/0         192.168.164.19  Et0/1         192.168.201.180 06 FA1C 557B     5
Et0/0         192.168.66.15   Et0/1         192.168.155.182 11 FBC6 585A     3
Et0/0         192.168.100.208 Et0/1         192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1         192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1         192.168.60.0    06 0FAA F001     1
Et0/0         192.168.29.205  Et0/1         192.168.240.249 11 71B3 8F9C     8
Et0/0         192.168.100.179 Et0/1         192.168.60.214  06 A2C4 F005     4
Et0/0         192.168.89.13   Et0/1         192.168.204.26  11 1D17 2CB0    11
router#
```

앞의 예에서는 다음과 같은 여러 플로우가 있습니다.

- TCP 포트 80의 HTTP(16진수 값 0050)
- TCP 포트 443의 SSL(16진수 값 01BB)
- TCP 포트 1100(16진수 값 044C)
- TCP 포트 8080(16진수 값 1F90)
- TCP 포트 8081(16진수 값 1F91)
- TCP 포트 8082(16진수 값 1F92)
- TCP 포트 8443(16진수 값 20FB)
- TCP 포트 8999(16진수 값 2327)
- TCP 포트 9000(16진수 값 2328)
- TCP 포트 9501(16진수 값 251D)
- TCP 포트 12102(16진수 값 2F46)
- TCP 포트 12104(16진수 값 2F48)
- TCP 포트 32000(16진수 값 7D00)
- TCP 포트 61441(16진수 값 F001)
- TCP 포트 61445(16진수 값 F005)
- UDP 포트 69의 TFTP(16진수 값 0045)

이 트래픽은 인프라 디바이스에 사용되는 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 위의 프로토콜/포트에서 전송된 트래픽의 기준 사용률과 비교하고, 플로우를 조사하여 신뢰할 수 없는 호스트 또는 네트워크에서 소싱되는지 확인하는 것이 좋습니다. 위의 포트/프로토콜에 있는 패킷에 대한 트래픽 흐름만 보려면 명령 show ip cache flow를 사용합니다 | include SrcIf|__11_.*0045는 다음과 같이 관련 UDP NetFlow 레코드를 표시합니다.

UDP 플로우

```
router#show ip cache flow | include SrcIf|_11_.*0045
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

Et0/0         192.168.54.222  Et0/1         192.168.60.43   11 7947 0045     3
Et0/0         192.168.247.117 Et0/1         192.168.60.169  11 45FB 0045     1
Et0/0         192.168.250.16  Et0/1         192.168.60.79   11 66AC 0045    10
```

```
Et0/0         192.168.121.112 Et0/1         192.168.60.36   11 6725 0045    16
Et0/0         192.168.243.192 Et0/1         192.168.60.225  11 2B52 0045     1
router#
```

위의 포트/프로토콜에 있는 패킷에 대한 트래픽 흐름만 보려면 명령 show ip cache flow를 사용합니다 | include SrcIf|__06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F005)_ 여기에 표시된 대로 관련 TCP NetFlow 레코드를 표시합니다.

TCP 흐름

```
router#show ip cache flow | include
SrcIf|_06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F0
05)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.100.14  Et0/1          192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1          192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.100.164 Et0/1          192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1          192.168.60.30   06 E440 1F92     6

Et0/0         192.168.100.211 Et0/1          192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1          192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1          192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2328     4

Et0/0         192.168.100.121 Et0/1          192.168.60.165  06 15A0 2F48     8

Et0/0         192.168.100.208 Et0/1          192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1          192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1          192.168.60.0    06 0FAA F001     1
Et0/0         192.168.100.179 Et0/1          192.168.60.214  06 A2C4 F005     4

Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
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 디바이스로 전송되는 다음 프로토콜/포트의 무단 패킷을 거부합니다.

- TCP 포트 80
- TCP 포트 443
- TCP 포트 1100
- TCP 포트 8080
- TCP 포트 8081

- TCP 포트 8082
- TCP 포트 8443
- TCP 포트 8999
- TCP 포트 9000
- TCP 포트 9501
- TCP 포트 12102
- TCP 포트 12104
- TCP 포트 32000
- TCP 포트 61441
- TCP 포트 61445
- UDP 포트 69

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 tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 80 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1100
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 8081 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 8082 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 9000 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 12102 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 12104 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 61441 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 access-list tACL-Policy extended permit udp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 69 ! !-- 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 80
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 1100
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 8081
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8082
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9501
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12102
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12104
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61441
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61445
```

```
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 69 ! !-- 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 다음 프로토콜/포트를 식별할 수 있습니다.

- TCP 포트 80
- TCP 포트 443
- TCP 포트 1100
- TCP 포트 8080
- TCP 포트 8081
- TCP 포트 8082
- TCP 포트 8443
- TCP 포트 8999
- TCP 포트 9000
- TCP 포트 9501
- TCP 포트 12102
- TCP 포트 12104
- TCP 포트 32000
- TCP 포트 61441
- TCP 포트 61445
- UDP 포트 69

관리자는 필터링된 패킷을 조사하여 이러한 취약성을 악용하려는 시도인지 확인하는 것이 좋습니다. show access-list tACL-Policy의 출력 예는 다음과 같습니다.

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 31 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www (hitcnt=55)
```

```
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq https (hitcnt=765)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=43)
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=265)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=18)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=77)
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=345)
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=137)
access-list tACL-Policy line 9 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=17)
access-list tACL-Policy line 10 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=36)
access-list tACL-Policy line 11 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=40)
access-list tACL-Policy line 12 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=23)
access-list tACL-Policy line 13 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=109)
access-list tACL-Policy line 14 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=60)
access-list tACL-Policy line 15 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=95)
access-list tACL-Policy line 16 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq tftp (hitcnt=4567)
access-list tACL-Policy line 17 extended deny tcp any
192.168.60.0 255.255.255.0 eq www (hitcnt=28)
access-list tACL-Policy line 18 extended deny tcp any
192.168.60.0 255.255.255.0 eq https (hitcnt=169)
access-list tACL-Policy line 19 extended deny tcp any
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=93)
access-list tACL-Policy line 20 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=11)
access-list tACL-Policy line 21 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=9)
access-list tACL-Policy line 22 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=9)
access-list tACL-Policy line 23 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=34)
access-list tACL-Policy line 24 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=46)
access-list tACL-Policy line 25 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=6)
access-list tACL-Policy line 26 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=9)
access-list tACL-Policy line 27 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=11)
access-list tACL-Policy line 28 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=24)
access-list tACL-Policy line 29 extended deny tcp any
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=48)
access-list tACL-Policy line 30 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=32)
access-list tACL-Policy line 31 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=9)
access-list tACL-Policy line 32 extended deny udp any
192.168.60.0 255.255.255.0 eq tftp (hitcnt=78)
```

```
access-list tACL-Policy line 33 extended deny ip any any (hitcnt=4658)
firewall#
```
앞의 예에서 액세스 목록 tACL-Policy는 신뢰할 수 없는 호스트 또는 네트워크에서 받은 다음 패킷을 삭제했습니다.

- ACE 라인 17의 TCP 포트 80(www)에서 28개의 HTTP 패킷
- ACE 라인 18용 TCP 포트 443(https)의 SSL 패킷 169개
- ACE 라인 19용 TCP 포트 1100의 93개 패킷
- ACE 라인 20용 TCP 포트 8080의 패킷 11개
- ACE 라인 21용 TCP 포트 8081의 패킷 9개
- ACE 라인 22용 TCP 포트 8082의 패킷 9개
- ACE 라인 23용 TCP 포트 8443의 34개 패킷
- ACE 라인 24용 TCP 포트 8999의 46개 패킷
- ACE 라인 25용 TCP 포트 9000의 패킷 6개
- ACE 라인 26용 TCP 포트 9501의 패킷 9개
- ACE 라인 27에 대한 TCP 포트 12102의 패킷 11개
- ACE 라인 28에 대한 TCP 포트 12014의 24개 패킷
- ACE 라인 29에 대한 TCP 포트 32000의 48개 패킷
- ACE 라인 30에 대한 TCP 포트 61441의 32개 패킷
- ACE 라인 31에 대한 TCP 포트 61445의 패킷 9개
- ACE 라인 32의 UDP 포트 69(tftp)에서 78개의 TFTP 패킷

식별: 방화벽 액세스 목록 Syslog 메시지

log 키워드가 없는 ACE(Access Control Entry)에서 거부된 패킷에 대해 방화벽 syslog 메시지 106023이 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. grep 키워드와 함께 다른 정규식을 사용하여 로깅된 메시지의 특정 데이터를 검색할 수 있습니다.

정규식 구문에 대한 추가 정보는 정규식 만들기에 있습니다.

```
firewall#show logging | grep 106023
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.215/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.173/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
```

```
                dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.225.47/1024
                dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.156.169/1024
                dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.191.223/1024
                dst inside:192.168.60.103/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                dst inside:192.168.60.25/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                dst inside:192.168.60.177/8080 by access-group "tACL-Policy"
firewall#
```

앞의 예에서 tACL tACL-Policy에 대해 로깅된 메시지는 영향을 받는 디바이스에 할당된 주소 블록으로 전송된 TCP 포트 80의 HTTP 패킷, TCP 포트 443의 SSL 패킷, TCP 포트 1100의 패킷 및 TCP 포트 8080의 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
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %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 있

습니다.

```
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 삭제했습니다. 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 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.

- 32719-0: Cisco Telepresence 인증되지 않은 원격 임의 명령 실행
- 33859-0: Cisco TelePresence 엔드포인트 CGI 명령 삽입
- 33860-0: Cisco TelePresence Multipoint Switch Java Servlet Access
- 33860-1: Cisco TelePresence Multipoint Switch Java Servlet Access
- 33861-0: Cisco TelePresence Recording Server 명령 실행 취약성

32719-0: Cisco Telepresence 인증되지 않은 원격 임의 명령 실행

Cisco IPS 버전 6.x 이상을 실행하는 센서에 대한 시그니처 업데이트 S550부터 이러한 취약성을 시그니처 32719/0(시그니처 이름: Cisco Telepresence Unauthenticated Remote Arbitrary Command Execution)으로 탐지할 수 있습니다. 시그니처 32719/0은 기본적으로 활성화되어 있으며 High severity 이벤트를 트리거하고 SFR(signature fidelity rating)이 90이며 **produce-alert**의 기본 이벤트 작업**으로 구성됩니다**.

시그니처 32719/0은 TCP 포트 8082를 사용하여 전송된 Cisco TelePresence 엔드포인트에서 인증되지 않은 원격 임의 명령 실행 취약성을 악용하려는 시도에서 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

33859-0: Cisco TelePresence 엔드포인트 CGI 명령 삽입

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S550부터 시그니처 33859-0(시그니처 이름: Cisco TelePresence Endpoint CGI 명령 삽입)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 33859/0은 기본적으로 활성화되어 있으며 High severity 이벤트를 트리거하고 SFR(signature fidelity rating)이 80이며 **produce-alert**의 기본 이벤트 작업**으로 구성됩니다**.

시그니처 33859/0은 TCP 포트 8082를 사용하여 전송된 Cisco TelePresence 엔드포인트에서 인증되지 않은 원격 임의 명령 실행 취약성을 악용하려는 시도에서 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

33860-0: Cisco TelePresence Multipoint Switch Java Servlet Access

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S550부터 시그니처 33860-0(시그니처 이름: Cisco TelePresence Multipoint Switch Java Servlet Access)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 33860/0은 기본적으로 비활성화되어 있으며, High Severity 이벤트를 트리거하고, SFR(Signature Fidelity Rating)이 75이며, 기본 이벤트 작업인 **produce-alert로 구성됩니다**.

시그니처 33860/0은 TCP 포트 8080을 사용하여 전송된 Cisco TelePresence Multipoint Switch에서 여러 Java 서블릿에 액세스하는 것을 탐지할 때 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

참고: 이 서명은 Cisco TelePresence Multipoint Switch가 아닌 디바이스에서 독창적으로 발생할 수 있습니다. 이러한 장치를 제거하기 위해서는 추가적인 조사가 필요하다.

33860-1: Cisco TelePresence Multipoint Switch Java Servlet Access

Cisco IPS 버전 6.x 이상을 실행하는 센서에 대한 시그니처 업데이트 S550부터 이러한 취약성을 시그니처 33860-1(시그니처 이름: Cisco TelePresence Multipoint Switch Java Servlet Access)에서 탐지할 수 있습니다. 시그니처 33860/1은 기본적으로 비활성화되어 있으며, High severity 이벤트를 트리거하고, SFR(signature fidelity rating)이 75이며, 기본 이벤트 작업인 **produce-alert로 구성됩니다**.

시그니처 33860/1은 TCP 포트 80을 사용하여 전송된 Cisco TelePresence Multipoint Switch에서 여러 Java 서블릿에 액세스하는 것을 탐지할 때 발생합니다. 이 서명의 실행은 이러한 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

참고: 이 서명은 Cisco TelePresence Multipoint Switch가 아닌 디바이스에서 독창적으로 발생할 수 있습니다. 이러한 장치를 제거하기 위해서는 추가적인 조사가 필요하다.

33861-0: Cisco TelePresence Recording Server 명령 실행 취약성

Cisco IPS 버전 6.x 이상을 실행하는 센서의 시그니처 업데이트 S550부터 시그니처 33861/0(시그니처 이름: Cisco TelePresence Recording Server Command Execution Vulnerability)으로 이러한 취약성을 탐지할 수 있습니다. 시그니처 33861/0은 기본적으로 활성화되어 있으며 High severity 이벤트를 트리거하고 SFR(signature fidelity rating)이 90이며 **produce-alert**의 기본 이벤트 작업**으로 구성됩니다**.

이 서명은 Cisco TelePresence Recording Server에서 특정 명령 실행 취약성을 악용하려는 시도를 탐지할 때 발생합니다. 이 취약성은 CVE-2011-0382에 추가로 설명되어 있습니다.

시그니처 33861/0은 메타 시그니처이며, 메타 시그니처가 트리거되도록 모든 시그니처가 트리거되어야 하는 여러 하위 시그니처(시그니처 ID 33861-1부터 33861-4까지)로 구성됩니다. 따라서 각 개별 하위 서명은 자체적으로 이벤트 작업이 없으므로 각각 정보 심각도 이벤트로 간주됩니다.

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.

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 트리거된 서명에 대해 riskRatingValue가 90보다 큰 이벤트 작업을 수행하는 기본 재정의를 통해 구현됩니다.

위험 등급 및 위협 등급 계산에 대한 자세한 내용은 위험 등급 및 위협 등급: IPS 정책 관리 간소화

를 참조하십시오.

Cisco 보안 모니터링, 분석 및 대응 시스템

식별: Cisco 보안 모니터링, 분석 및 대응 시스템 사고

Cisco Security MARS(Monitoring, Analysis, and Response System) 어플라이언스는 IPS 서명을 사용하여 이 문서에 설명된 취약성과 관련된 이벤트와 관련된 인시던트를 생성할 수 있습니다.

- 32719-0: Cisco Telepresence 인증되지 않은 원격 임의 명령 실행
- 33859-0: Cisco TelePresence 엔드포인트 CGI 명령 삽입
- 33860-0: Cisco TelePresence Multipoint Switch Java Servlet Access
- 33860-1: Cisco TelePresence Multipoint Switch Java Servlet Access
- 33861-0: Cisco TelePresence Recording Server 명령 실행 취약성

S550 동적 서명 업데이트를 다운로드한 후, 각 IPS 서명 ID에 대해 다음 키워드를 사용하고 Cisco Security MARS 어플라이언스에서 **모든 Matching Event Raw Messages**의 쿼리 유형을 사용하면 IPS 서명으로 생성된 인시던트를 나열하는 보고서가 제공됩니다.

- **NR-32719/0** for IPS signature 32719/0
- **NR-33859/0** for IPS signature 33859/0
- **NR-33860/0** for IPS signature 33860/0
- **NR-33860/1** for IPS signature 33860/1
- **NR-33861** for IPS signatures 33861/0 ~ 33861/4

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 이벤트가 쿼리 및 보고서에서 알 수 없는 이벤트 유형으로 나타납니다. 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 Help(도움말) > About(정보)을 선택하고 IPS Signature Version(IPS 서명 버전) 값을 검토하여 MARS에서 다운로드한 현재 서명 버전을 확인할 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 릴리스에 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 것은 귀하의 책임입니다. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

개정 이력

개정 1.1	2011년 2월 25일	서명 ID 33861-0에 대한 정보를 포함하도록 업데이트되었습니다.
개정 1.0	2011년 2월 23일	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 TelePresence 강화 가이드
- Cisco Applied Mitigation 게시판
- Cisco 보안
- Cisco Security IntelliShield Alert Manager Service
- 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
- Cisco IOS의 보안 툴 명령 언어
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- Cisco ACE Application Control Engine 모듈 설명서
- 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.