Remediate Catalyst SD-WAN Security Advisory - 2026년 6월

목차

소개

이 문서에서는 2026년 6월 4일자 PSIRT 권고 사항을 기반으로 SD-WAN의 중요한 보안 취약성을 식별하고 해결하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst SD-WAN 아키텍처 및 제어 구성 요소(vManage, vSmart, vBond)
- Cisco Catalyst SD-WAN 업그레이드 절차
- Cisco TAC 케이스 관리 및 관리 기술 수집 절차

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

자세한 배경 정보 및 최신 업데이트는 공식 PSIRT 자문 페이지를 참조하십시오.

이러한 권고 사항은 다음 링크에서 확인할 수 있습니다.

- Cisco Catalyst SD-WAN Manager 인증 권한 에스컬레이션 취약성

이러한 결함은 다음 PSIRT 권고에 의해 해결됩니다.

- Cisco 버그 ID CSCwu18563

리미디에이션 워크플로 개요

이 권고 사항에서는 netadmin 권한을 익스플로잇해야 하는 SD-WAN Manager의 권한 에스컬레이션 취약성에 대해 설명합니다.

권고에 따르면, 인증되지 않은 원격 공격자가 이러한 권한을 얻기 위한 알려진 경로는 CVE-2026-20182(cisco-sa-sdwan-rpa2-v69WY2SW) 또는 CVE-2026-20127(cisco-sa-sdwan-rpa-EHchtZk) 익스플로잇입니다.

제어 구성 요소가 두 권고 사항에 대해 고정 릴리스로 업그레이드되었고 Cisco가 이전 이벤트에 제공한 관리 기술 파일에서 잠재적 IoC(Indicators of Compromise)를 식별하지 못한 경우, 검토된 파일에 따라 이 새로운 취약성에 대한 알려진 인증되지 않은 익스플로잇 경로가 해당 특정 디바이스에서 완화됩니다.

이렇게 해도 공격자가 유효한 netadmin 자격 증명을 보유하는 경우에는 문제가 발생하지 않습니다. Cisco는 이 취약성에 대한 소프트웨어 수정을 아직 발표하지 않았으며 해결 방법이 없습니다. 자세한 지침은 추후 제공될 예정입니다.

필요한 조치: 이 보안 권고 사항을 해결하기 위해 Cisco TAC 케이스를 엽니다.

TAC는 다음과 같은 경우에 사용할 수 있습니다.

- 보안 침해 지표에 대한 환경 평가
- 평가를 기반으로 적절한 교정 경로를 안내합니다.
- IOC(Indicators of Compromise: 보안 침해 지표)가 확인될 경우 취해야 할 다음 단계에 대한 지침 제공

1. Collect Admin-Techs(관리자-기술 수집) - 모든 제어 구성 요소(vSmart, vManage, vBond)에

서 admin-tech를 실행합니다. vSmart admin-techs는 동시에 실행할 수 없습니다. 한 번에 하나씩 실행하십시오. 다른 모든 항목은 어떤 순서로든 수집할 수 있습니다. Log and Tech(로그 및 기술) 옵션을 선택합니다. 코어가 필요하지 않습니다.
2. TAC 케이스 열기 - Cisco TAC에 문의하고 모든 제어 구성 요소 관리 기술 로그 번들을 제공합니다.
3. TAC 평가- 환경 내 IOC(Indicators of Compromise)에 대한 사전 평가를 실시하고 TAC에서 해당 환경의 IOC(Indicators of Compromise)에 대한 사전 평가를 실시합니다.
4. 교정 실행 - 필요한 경우 TAC에서 제공하는 특정 프로세스를 완료합니다.

1단계: 모든 제어 구성 요소에서 Admin-Tech 파일 수집

필수: 진단 데이터 및 잠재적 IoC(indicators of compromise, 보안 침해 지표)가 보존되도록 업그레이드 또는 컨피그레이션 변경 전에 모든 제어 구성 요소에서 admin-tech 파일을 수집합니다. 이러한 파일은 3단계에서 TAC에서 사용자 환경을 분석하는 데 사용됩니다.

수집: admin-tech 생성의 경우 Log and Tech options를 선택합니다. 코어가 필요하지 않습니다.

1. 모든 컨트롤러(vSmarts)에서 admin-tech 실행 — 이러한 작업을 동시에 실행하지 마십시오. 한 번에 하나씩 수집
2. 모든 관리자에서 admin-tech 실행(vManages)
3. 모든 유효성 검사기에서 admin-tech 실행(vBonds)

SD-WAN 환경에서 관리 기술 수집 및 TAC 케이스에 업로드

참고: TAC에서는 이러한 파일을 분석하여 해당 조언과 관련된 보안 침해 지표를 귀사의 환경에 평가합니다. 이 권고에 대한 분석은 합법적인 사용과 악의적인 사용을 구분하지 않는 특정 로그 항목에 중점을 둡니다. TAC의 수동 검토가 필요합니다.

대체 방법: 수동 확인(Admin-Tech를 수집할 수 없는 경우에만)

admin-tech 파일을 공유할 수 없는 고객의 경우 수동 확인 단계를 사용할 수 있습니다. 이 단계에서는 문서화하고 TAC와 공유해야 하는 예비 지표를 제공합니다.

자세한 절차는 이 문서의 끝에 있는 수동 확인 단계 섹션을 참조하십시오. 모든 조사 결과를 문서화하고 지원 사례에서 TAC에 제공하십시오.

2단계: TAC 케이스 열기 및 Admin-Tech 파일 업로드

1단계에서 admin-tech를 수집한 후 Cisco TAC 지원 사례를 열고 수집한 admin-tech 파일을 업로드합니다. TAC는 이 권고와 관련된 보안 침해 지표를 확인하기 위해 관리자-기술을 분석합니다.

필요한 작업:

1. 제목의 "CVE-2026-20245" 및 권고 ID `cisco-sa-sdwan-privesc-4uxFrdzx`가 포함된 심각도 3 TAC 케이스를 열어 분석을 시작합니다.
2. 1단계에서 수집된 모든 admin-tech 로그 번들(컨트롤러, 관리자 및 검사기)을 업로드합니다.
3. TAC에서 분석을 완료하고 결과를 전달할 때까지 기다립니다.

참고: Cisco는 이 취약성에 대한 소프트웨어 수정을 발표하지 않았으며 해결 방법이 없습니다. 3단계의 TAC 분석을 통해 제공된 관리 기술 파일에 보안 침해 지표가 있는지 여부를 확인할 수 있습니다. 엔지니어링 팀에서 추가 지침을 제공할 예정입니다.

3단계: TAC 평가

TAC는 2단계에서 업로드한 관리 기술 파일의 사전 분석을 수행하고 이러한 파일에 대해 이 권고와 관련된 보안 침해 지표를 평가합니다.

이 권고에서는 각 관리자(vManage)의 /var/log/scripts.log에 있는 특정 로그 항목에 대해 중점적으로 분석합니다. 기본 명령이 적법하고 로그는 적법한 사용과 악의적인 사용을 구분하지 않으므로, 일치하는 엔트리는 확인 지표로 취급되기 전에 고객의 정상적인 운영 상태에 대한 TAC의 수동 검토가 필요합니다.

TAC 분석의 가능한 결과:

- 일치하는 로그 항목이 식별되지 않음 - 검토한 관리 기술 파일을 기반으로 이 권고 사항과 관련된 지표가 관찰되지 않았습니다. 현재 이 권고 사항에 대한 추가 조치가 필요하지 않습니다. 결과는 수신된 admin-tech 파일로 제한되며 각 디바이스의 로그 보존 기간에 의해 제한될 수 있습니다.
- 일치하는 로그 항목 확인 - TAC에서 추가 검토 단계를 통해 고객과 접촉 Cisco는 이 권고에 대한 소프트웨어 수정을 릴리스하지 않았기 때문에 업그레이드만으로 이 취약성이 해결되지는 않습니다. 확인된 감염 시나리오에 대한 TAC 지침은 4단계에서 참조된 관련 TechZone 문서에 문서화됩니다.

참고: 권고 사항에 따라 이 취약성을 악용하려면 netadmin 권한이 필요합니다. 즉, 인증되지 않은 공격자는 유효한 자격 증명이나 CVE-2026-20182 또는 CVE-2026-20127의 악용을 통해서만 얻을 수 있습니다. 제어 구성 요소가 이러한 권고 사항에 대해 모두 고정 릴리스로 업그레이드되고 이전 이벤트에 대한 보안 침해 지표가 식별되지 않은 경우, 검토된 파일에 따라 이 새로운 취약성에 대한 알려진 인증되지 않은 익스플로잇 경로가 해당 특정 디바이스에서 완화됩니다.

4단계: IoC(Indicators of Compromise, 보안 침해 지표)가 확인된 경우 — TAC 지침 준수

TAC에서 해당 환경에서 이 권고와 관련된 보안 침해 지표를 식별하면 TAC에서 구체적인 지침을

제공합니다. TAC에서 제공하는 모든 지침을 완료합니다.

이 권고 사항에 대해 보안 침해 지표가 식별되지 않은 경우, 검토된 관리 기술 파일을 기준으로 현재 이 권고 사항에 대한 추가 조치가 필요하지 않습니다.

⚠ 중요: Cisco는 이 권고에 대한 소프트웨어 수정을 릴리스하지 않았으며 해결 방법이 없습니다. 이 취약성을 악용하려면 CVE-2026-20182 또는 CVE-2026-20127을 통해 얻은 netadmin 권한이 필요하므로, 고객은 이러한 사전 권고의 교정이 완료되었는지 확인해야 합니다. 설정된 교정 흐름에 대해서는 해당 문서를 참조하십시오.

고려 사항

성공적인 교정이 끝나면 각 고객의 구체적인 보안 보증 요구 사항에 따라, 고객은 다음과 같은 위생 활동을 평가하고 이행하기를 원할 수 있습니다. 이러한 활동은 어떤 교정 옵션을 선택했는지에 관계없이 적용됩니다. 고객이 직접 관리하며 Cisco는 고객을 대신하여 직접 또는 수행하지 않습니다.

- 모든 로컬 사용자 계정 검토
- 자격 증명 회전
- 디바이스 컨피그레이션에 있는 모든 비밀의 회전(예: 완전한 목록이 아닌 목록):
  - 로컬 사용자 계정에 대한 자격 증명
  - SNMP 커뮤니티 문자열
  - TACACS 비밀 키
  - VPN 사전 공유 키 및 인증서
  - 신뢰할 수 있는 SSH 키
- 구성 템플릿 검토

엣지 디바이스 — 보안 침해로 의심되는 디바이스

Cisco는 특정 교정 경로를 권장하지 않습니다. 리미디에이션 옵션의 선택은 고객의 책임입니다. 환경을 평가하는 고객을 위한 정보 참고 사항: 고객이 엣지 장치의 손상을 의심할 경우, 영향을 받는 엣지 장치의 출고 시 리셋 및 재온보딩은 고객이 선택할 때 고려하고자 하는 고객 관리 조치입니다. 이러한 접근 방식의 추구 여부 및 선택할 수 있는 선택권은 고객에게 있다.

보안 공장 재설정을 수행하는 적절한 명령은 다음과 같습니다.

```
factory-reset all secure 3-pass
```

고정 소프트웨어 버전

⚠ 중요: 이 문서의 발행 시점에 Cisco는 CVE-2026-20245를 해결하는 소프트웨어 픽스를 발표하지 않았습니다. Cisco는 향후 릴리스에서 Cisco Catalyst SD-WAN Manager의 이러한 취약성을 해결할 계획입니다. 해결 방법이 없습니다. 이 섹션은 고정 소프트웨어를 사용할 수 있게 되면 업데이트됩니다.

이 취약성을 악용하려면 인증되지 않은 공격자가 CVE-2026-20182 또는 CVE-2026-20127을 통해서만 얻을 수 있는 netadmin 권한이 필요하므로, 고객은 제어 구성 요소가 그러한 사전 권고에 대한 고정 릴리스를 실행하고 있는지 확인하는 것이 좋습니다. 이러한 권고에 대한 고정 릴리스는 2026년 5월 14일 SD-WAN Security Advisory 및 해당 TechZone 문서에 나와 있습니다.

- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability(2026년 5월 14일)
- (고정 소프트웨어 버전 테이블)

중요 참조:

- 업그레이드 매트릭스
- 컨트롤러 호환성 매트릭스

부록: 수동 확인 단계(Admin-Tech 수집이 불가능한 경우에만)

✎ 참고: Admin-tech 수집이 기본 설정 방법입니다. 관리 기술 파일을 수집하고 TAC와 공유할 수 없는 경우에만 아래의 수동 확인 단계를 사용하십시오. 이 수동 단계의 결과는 예비 단계입니다. 조사 결과를 문서화하고 공식 평가를 수행하는 TAC와 공유합니다.

✎ 참고: 이 권고의 경우 수동 확인은 단일 대상 로그 확인으로 구성됩니다. 검색된 로그 항목은 합법적인 명령에 의해 생성되며 로그만은 합법적인 사용과 악의적인 사용을 구분하지 않습니다. 일치하는 엔트리는 잠재적 지표로 취급되기 전에 고객의 정상적인 작동 상태를 기준으로 검토해야 합니다. 일치하는 항목을 정상 운영과 조정할 수 없는 경우, 검색 결과를 문서화하고 TAC와 공유합니다.

확인: 테넌트 목록 업로드 항목에 대해 각 관리자(vManage)에서 scripts.log를 확인합니다.

PSIRT 권고에 따라 고객은 `/var/log/`에 있는 `scripts.log` 파일에 대해 다음 예와 유사한 항목을 감사하는 것이 좋습니다.

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

1단계: 각 관리자(vManage)에서 vshell에 액세스하고 로그 파일을 검색합니다.

vManage CLI에서 vshell로 드롭하고 다음을 실행합니다.

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

구축의 모든 vManage(모든 클러스터 멤버 및 DR 쌍 vManage 포함)에서 검사를 반복합니다.

2단계: TAC용 결과 및 문서 해석

일치하는 엔트리가 반환되지 않는 경우

- 이 경고와 관련된 보안 침해 지표는 이 디바이스의 로그 파일에서 관찰되지 않았습니다.
- 이 결과를 TAC 케이스에 문서화합니다(디바이스 호스트 이름 및 검색한 로그 파일의 날짜/범위 포함).
- 나머지 Manager에 대한 검사를 계속합니다.

일치하는 항목이 반환되는 경우:

- 일치하는 각 항목은 고객의 정상적인 운영 상태를 기준으로 검토해야 합니다. 기본 명령(테넌트 목록 업로드)은 합법적이며 루틴 작업 중에 나타날 수 있습니다.
- 일치하는 각 항목에 대해 타임스탬프, 전체 로그 줄 및 cli 경로 뒤에 참조되는 파일 경로를 캡처합니다.
- 일치하는 항목을 알려진 합법적 작업으로 검증할 수 없는 경우 이 항목은 보안 침해 지표가 될 수 있습니다. 결과를 문서화하고 검토를 위해 TAC에 제공합니다.
- 모든 조사 결과를 문서화하고 TAC 케이스를 엽니다. 경우에 따라 일치하는 로그 항목과 source 명령 출력을 포함합니다.
- TAC에서 공식 평가 수행 평가에서 IOC가 확인된 경우 관련 TechZone 문서에 설명된 흐름을 따릅니다. 및 리미디에이션 가이드입니다.

자주 묻는 질문(FAQ)

Q: 이 보안 권고 사항을 해결하기 위한 첫 번째 단계는 무엇입니까?

A : 업그레이드 또는 컨피그레이션 변경 전에 모든 제어 구성 요소(vSmart, vManage, vBond)에서 admin-tech 파일을 수집하여 진단 데이터 및 잠재적 보안 침해 지표를 보존합니다. 그런 다음 Cisco TAC 케이스를 열고 TAC에서 분석할 수 있도록 admin-techs를 업로드합니다.

Q: Cisco에서 이 취약성에 대한 소프트웨어 수정을 릴리스했습니까?

A : 이 문서의 발행 당시에는 그렇지 않습니다. 이 권고에 따라 Cisco는 향후 릴리스에서 Cisco Catalyst SD-WAN Manager의 이러한 취약점을 해결할 계획입니다. 해결 방법이 없습니다. 이 문서는 고정 릴리스를 사용할 수 있게 되면 업데이트됩니다.

Q: 해결책이 없는 경우 Cisco에서 지금 어떤 조치를 권장하는 이유는 무엇입니까?

A : 이 취약성을 악용하려면 netadmin 권한이 필요합니다. 권고 사항에 따라 인증되지 않은 공격자는 유효한 자격 증명 또는 CVE-2026-20182 또는 CVE-2026-20127의 익스플로잇을 통해서만 이러한 권한을 얻을 수 있습니다. 이러한 이전 권고 사항에 대한 제어 구성 요소가 고정 릴리스로 업그레이드되어 이 취약성을 공격하는 데 필요한 권한을 얻는 데 알려진 인증되지 않은 경로를 해결합니다. 3단계의 admin-tech 분석을 통해 검토된 파일에 보안 침해 지표가 있는지 여부를 확인할 수 있습니다.

Q: 모든 제어 구성 요소에서 admin-techs를 수집해야 합니까?

A : 예. TAC에서는 모든 컨트롤러(vSmart, 한 번에 하나씩 수집됨), 모든 관리자(vManage) 및 모든 검증자(vBond)의 관리 기술 파일이 분석을 수행해야 합니다.

Q: TAC는 시스템에 이 조언과 관련된 IOC가 있는지 어떻게 확인합니까?

A : TAC는 관리 기술 파일을 검토하고 각 관리자의 PSIRT 권고 사항(/var/log/scripts.log)에 설명된 특정 로그 항목을 찾습니다. 기본 명령은 합법적입니다. 일치하는 엔트리는 잠재적인 지표로 취급되기 전에 정상적인 작동 상태를 기준으로 검토해야 합니다. TAC에서 검토를 수행합니다.

Q: 보안 침해 지표가 식별되면 어떻게 됩니까?

A : TAC에서 구체적인 지침을 제공합니다. 현재 이 권고에 사용할 수 있는 소프트웨어 수정 사항이 없으므로 업그레이드만으로 확인된 보안 침해가 해결되지는 않습니다. TAC의 지침은 2026년 5월 및 2026년 2월 자문에 대한 관련 TechZone 문서에 설명된 흐름을 따릅니다.

Q: 에지 라우터(Cisco IOS XE)는 이 권고의 영향을 받습니까?

A : 이 권고는 Cisco Catalyst SD-WAN Manager에 영향을 미칩니다. 권고에 따르면 Cisco는 이 취약성을 악용하여 에지 디바이스에 가해지는 컨피그레이션 변경을 초래한 제한된 사례를 관찰했습니다. 고객은 에지 디바이스의 컨피그레이션을 확인하는 것이 좋습니다.

Q: 어떤 구축 유형이 영향을 받습니까?

A : 권고에 따르면, 이 취약성은 온프레미스 구축, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud(Cisco Managed), Cisco SD-WAN Cloud for Government(FedRAMP) 등 디바이스 구성에 관계없이 모든 Cisco Catalyst SD-WAN Manager 구축 유형에 영향을 미칩니다.

Q: 나는 이미 2026년 5월과 2026년 2월에 대한 권고를 업그레이드했으며 이러한 이벤트에 대한 보안 침해 지표가 확인되지 않았습니다. 제가 이 새로운 취약성에 노출되었습니까?

A : 제어 구성 요소가 CVE-2026-20182 및 CVE-2026-20127 모두에 대해 고정 릴리스를 실행하고 있고 검토된 관리 기술 파일에서 이전 이벤트에 대한 보안 침해 지표가 식별되지 않은 경우, 검토된 파일을 기반으로 이 새로운 취약성에 대한 알려진 인증되지 않은 익스플로잇 경로가 해당 특정 디바이스에서 완화됩니다. 이렇게 해도 공격자가 유효한 netadmin 자격 증명을 보유하는 경우의 노출이 사라지지 않습니다.

Q: TAC를 기다리지 않고 직접 검증을 수행할 수 있습니까?

A : admin-techs를 공유할 수 없는 고객은 부록에 설명된 수동 확인 단계를 수행할 수 있습니다. 그

결과는 예비; 조사 결과를 문서화하고 공식 평가를 수행하는 TAC와 공유합니다.

Q: SD-WAN 오버레이를 강화하기 위한 일반적인 모범 사례는 무엇입니까?

A : 모범 사례는 Cisco Catalyst SD-WAN 강화 가이드를 참조하십시오.

Q: Cisco TAC는 이 취약성에 대한 포렌식 분석 또는 조사 서비스를 제공합니까?

A : Cisco TAC는 PSIRT 권고에 문서화된 보안 침해 지표에 대한 관리 기술 파일을 검토하여 고객을 지원할 수 있습니다. Cisco TAC는 심층 포렌식 분석 또는 사고 조사를 수행하지 않습니다. 포괄적인 포렌식 작업 또는 세부적인 보안 조사를 위해 고객은 선호하는 서드파티 IR(Incident Response) 회사를 이용하는 것이 좋습니다.

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.