

이미 존재하는 문서에 대해 굵게 확인

목차

[소개](#)

[참조 — Cisco SD-WAN CVE-2026-20182 설명서](#)

[이메일](#)

[Sherlock 1 - Intake - 업그레이드 요청 및 Admin-Tech 파일](#)

[Sherlock 2 - 결과 - 관찰된 IoC 없음\(파일당\)](#)

[설록 3 - 알림 - Admin-Tech 파일 누락](#)

[TAC 1 - 조사 - 추가 검토 필요\(IoC 의심\)](#)

[TAC 2 - 결과 - IoC를 찾을 수 없음\(엔지니어 확인\)](#)

[TAC 3 - 검증 - 오버레이의 IP 소유권 확인](#)

[TAC 4 - 결과 - 오답 제거됨](#)

[TAC 5 - 중요 - IoC 식별, 검토 통화 일정 예약](#)

[TAC 6 - 결과 - 중복 IoC\(닫기 및 리디렉션\)](#)

[TAC 7 - 리미디에이션 - 옵션 후속 조치\(통화 후\)](#)

[TAC 8 - 교정 - 손상된 패브릭에 대한 업데이트된 옵션\(옵션 2 후속 조치\)](#)

[TAC 17 - 역조사 결과 - 이전에는 IoC가 없었고, 이제 IoC가 식별됨\(CVE-2026-20182\)](#)

[CloudOps 1 - 사전 대응적 - 클라우드 스캔에서 탐지된 IoC, 검증을 위해 필요한 관리 기술](#)

[옵션 A, B 또는 C를 아직 완료하지 않은 이전에 영향을 받은 고객을 위한 WAVE 2A 이메일. \(옵션 1과 2를 다시 수행해야 함\)](#)

[PSIRT2a에 대한 IOC 없음을 위한 TAC 9 템플릿/재구축함\(이전에 영향 받음\)](#)

[PSIRT2a에 대한 IOC의 TAC 10 템플릿/재구축 완료\(이전 영향\)](#)

[PSIRT2a에 대한 IOC 없음을 위한 TAC 11 템플릿/재구축하지 않음\(이전에 영향 받음\)](#)

[PSIRT2a의 IOC에 대한 TAC 12 템플릿/재구축하지 않음\(이전에 영향 받음\)](#)

[신규 고객을 위한 WAVE 2A 이메일\(이전에는 영향 받지 않음\)](#)

[IOC 없음/사용 가능한 고정 릴리스 없음을 위한 TAC 13 템플릿\(WAVE 2a — Await Fix\)](#)

[IOC/고정 릴리스를 사용할 수 없는 TAC 14 템플릿\(WAVE 2a — 지금 업그레이드\)](#)

[IOC 식별/고정 릴리스용 TAC 15 템플릿 사용 가능\(WAVE 2a — 긴급 업그레이드\)](#)

[IOC용 TAC 16 템플릿 식별/사용 가능한 고정 릴리스 없음\(WAVE 2a — 고정 및 대기 수정\)](#)

소개

이 문서에서는 Cisco Catalyst SD-WAN Controller Authentication Bypass 취약성과 관련된 케이스 분류 및 교정 중에 사용되는 승인된 고객 이메일 템플릿을 중앙 집중화합니다. Sherlock(관리 기술 데이터를 수집하고 예비 IoC 결과를 반환하는 자동화된 케이스 교환) 및 TAC 엔지니어(조사, 검증, 교정 지침을 위한 사람 중심 후속 조치)와 같이 발신자별로 템플릿이 분할됩니다.

[참조 — Cisco SD-WAN CVE-2026-20182 설명서](#)

위의 이메일 템플릿에서 참조된 모든 Cisco 문서의 마스터 목록입니다. 번호 지정은 이메일별 수퍼스크립트 (예: [2]) 이 목록의 항목을 가리킵니다.

1. Cisco SD-WAN 강화 가이드 — <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. 공식 보안 자문(cisco-sa-sdwan-mltnps2-JxpWm7R) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. TAC 리미디에이션 가이드 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-hld--1516256622>
4. Cisco SD-WAN 업그레이드 가이드 — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. Cisco SD-WAN 관리 기술 수집 가이드 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. 2차 보안 자문(cisco-sa-sdwan-rpa2-v69WY2SW) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. Catalyst SD-WAN 업그레이드 시작 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

이메일

Sherlock 1 - Intake - 업그레이드 요청 및 Admin-Tech 파일

사용 사례

CVE-2026-20182에 대한 TAC 케이스가 열려 모든 SD-WAN 제어 구성 요소에서 관리-기술 데이터를 수집한 다음 업그레이드하는 것이 권장되는 초기 지원

제목

중요: CVE-2026-20182에 필요한 조치 - 업그레이드 계획 및 IoC 평가

메시지

고객님,

Cisco TAC(Technical Assistance Center)에 문의해 주셔서 감사합니다.

CVE-2026-20182와 관련된 취약성과 관련하여 자세한 내용은 [공식 보안 권고](#)^[1] 및 [TAC 교정 가이드](#)^[2]를 참조하십시오.

Cisco의 1차 목표는 고객의 환경을 보호하는 것입니다. 이 위험을 **완화하기 위한** 가장 중요한 단계로 **업그레이드 계획 및 실행**의 우선 순위를 지정해 주십시오. 아직 이 업그레이드를 예약하지 않으셨다면 즉시 예약해 주십시오.

업그레이드 리소스: 업그레이드 수행 방법에 대한 자세한 지침은 다음 Cisco 공식 문서를 참조하십시오. [Cisco SD-WAN 업그레이드 가이드](#)^[3]

CVE-2026-20182와 관련된 잠재적 IoC(Indicators of Compromise)에 대한 환경 초기 평가를 활성화하려면 업그레이드 전에 admin-tech 수집을 수행해야 합니다. 다음 작업 순서를 따르십시오.

- Admin-Tech 파일 수집:** 업그레이드 전에 모든 SD-WAN 제어 구성 요소에서 admin-tech 로그를 생성하여 진단 데이터가 손실되지 않도록 합니다. 이러한 파일을 생성할 때 **"Logs"** 및 **"Tech"**를 모두 선택해야 합니다.
 - **vSmarts(컨트롤러):** 동시에 수집하지 말고 한 번에 하나씩 수집하십시오.
 - **vBonds(유효성 검사기):** 모든 노드에서 수집합니다.
 - **관리자(vManage):** 클러스터의 모든 노드(활성 및 대기 DR)에서 수집합니다.
- 업그레이드 실행:** 모든 SD-WAN 제어 구성 요소(vManage, vSmart, vBond)를 권고에 나열된 고정 소프트웨어 버전으로 업그레이드합니다. 업그레이드를 시작하기 전에 admin-tech 로그 분석을 기다리지 마십시오. 업그레이드로 인해 취약성이 즉시 닫힙니다.
- TAC 케이스에 업로드:** 업그레이드가 완료되면, 가능한 경우 이전에 수집한 파일을 기존 TAC 케이스에 동시에 업로드합니다. 그런 다음 Cisco 팀은 이러한 로그를 스캔하여 IoC(Indicators of Compromise: 보안 침해 지표)에 대한 귀사의 환경을 평가합니다.

리소스 및 지원:

관리 기술 파일을 생성하고 안전하게 제출하는 방법에 대한 자세한 내용과 단계별 지침은 다음 가이드를 참조하십시오. [Cisco SD-WAN 관리 기술 수집 가이드](#)^[4].

BCS/LCS 서브스크립션이 있는 경우 Cisco NCE 또는 Delivery Manager에 문의하여 업그레이드 프로세스 또는 다음 단계에 대한 추가 지침을 확인하십시오.

귀하의 데이터 프라이버시 및 보안은 당사의 최우선 과제로 남아 있습니다. 제공된 모든 정보는 Cisco의 개인정보 보호 및 보안 정책에 따라 처리됩니다.

케이스에 성공적으로 업로드된 각 파일에 대한 자동 이메일 확인 메시지를 받게 됩니다. 이 알림을 검토하십시오.

인프라 보안에 대한 신속한 협력에 감사드립니다.

링크:

- [1] [공식 보안 자문](#)
- [2] [TAC 리미디에이션 가이드](#)
- [3] [Cisco SD-WAN 업그레이드 가이드](#)
- [4] [Cisco SD-WAN 관리 기술 수집 가이드](#)

감사합니다.

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

Sherlock 2 - 결과 - 관찰된 IoC 없음(파일당)

사용 사례

관리 기술 분석 후 전송됨: 업로드된 특정 파일에 대해 관찰된 보안 침해 지표가 표시되지 않습니다. 처리된 파일당 한 번 전송됨.

제목

Update: SD-WAN 구성 요소에 대한 분석 결과 [파일 이름 삽입] - CVE-2026-20182

메시지

고객님,

기다려 주셔서 감사합니다.

admin-tech 파일 [Insert File Name] 분석을 완료했습니다. 해당 파일 내에서 이 특정 장치에 대한 CVE-2026-20182 관련 보안 침해 지표를 식별하지 못했습니다.

이 검토를 위해 Cisco에 검색 및 제공한 로그 데이터의 양은 **Cisco SD-WAN 강화 가이드**^[1]에 따라 구성

한 로그 보존 기간에 의해 제한될 수 있습니다.

중요: 다음 단계 및 케이스 마감:

1. **모든 결과 대기:** 이 이메일의 결과는 부분적인 결과일 수 있습니다. 우리는 제공된 대로 각 파일을 분석할 것입니다. 평가를 완료하기 전에 업로드된 모든 파일에 대한 확인을 받을 때까지 기다려 주십시오.
2. **업그레이드 우선 순위:** 관리자 기술 로그의 예비 검사에서 IoC(indicators of compromise)가 식별되지 않았지만 근본적인 취약성이 남아 있을 수 있습니다. Cisco Cloud-Pro 및 Cisco On-Prem 구축의 경우, 아직 하지 않았다면 가능한 한 빨리 SD-WAN 제어 구성 요소의 전체 업그레이드에 우선 순위를 지정해 주십시오.
 - Cisco 클라우드(fka: SaaS(Customer Fabric))는 Cisco가 관리 서비스의 일부로 자동 업그레이드합니다. 별도의 조치가 필요하지 않습니다.
3. **케이스 마감:** 업로드한 모든 파일에 대한 "관찰된 IoC 없음" 결과를 수신하고 (해당되는 경우) 환경 전체에서 소프트웨어 업그레이드를 성공적으로 완료한 경우, 이 케이스를 해결한 것으로 간주하고 표준 마감 절차를 진행할 수 있습니다.

업그레이드 리소스(해당되는 경우): Cisco Cloud-Pro 및 Cisco On-Prem의 업그레이드 수행 방법에 대한 자세한 지침은 다음 Cisco 공식 문서를 참조하십시오. Cisco SD-WAN 업그레이드 가이드

업그레이드 프로세스에 대한 개괄적인 개요는 다음과 같습니다.

1. 관리자(vManage) 리포지토리에 적절한 소프트웨어 이미지를 업로드합니다.
2. Manager(vManage)부터 시작하여 Validator(vBond) 및 Controller(vSmart)를 차례로 업그레이드합니다.
3. 새 소프트웨어 버전 활성화 및 시스템 기능 확인

우리는 당신의 사례를 계속 모니터링 할 것입니다. 귀사로부터 받은 파일을 토대로 모든 결과를 제공한 후 10일(영업일 기준) 이내에 회신을 받지 못한 경우 추가 지원이 필요하지 않다고 가정하고 정상적인 TAC 케이스 마감 절차를 진행합니다. 언제든지 도움이 필요하시면 저희에게 알려주세요

감사합니다.

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

사용 사례

제출된 admin-tech 파일이 로그에서 발견된 SD-WAN 제어 구성 요소 수와 일치하지 않을 경우 자동화된 후속 조치를 수행합니다.

제목

알림: CVE-2026-20182 평가에 필요한 Admin-Tech 파일 누락

메시지

고객님,

SD-WAN 제어 구성 요소에서 admin-techs가 여전히 누락되어 있으므로 시스템에서 admin-tech 로그의 Indicators of Compromise를 평가할 수 없습니다. CVE-2026-20182 평가를 시작하려면 클러스터링된 모든 Manager(vManage) 노드를 포함하여 모든 컨트롤러(vSmarts), Validator(vBonds) 및 Manager(vManage)로부터 관리 기술 파일을 수신해야 합니다.

다음 단계:

가능한 한 빨리 나머지 admin-tech 파일을 업로드하십시오.

감사합니다.

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(본문 포함)

↓ 다운로드 .eml 템플릿

TAC 1 - 조사 - 추가 검토 필요(loC 의심)

사용 사례

자동화를 통해 감염 가능성을 알려주는 로그가 발견되고 인적 조사가 필요한 경우 TAC 엔지니어가 보냅니다.

제목

SR# - 추가 조사 필요

메시지

고객님,

내 이름은 {your_name}이며 귀하의 케이스를 수락했습니다. Cisco TAC(Technical Assistance Center)에 지속적으로 협력해 주셔서 감사합니다.

SD-WAN 제어 구성 요소에서 제공한 admin-tech 파일을 사전에 분석한 후, 분석을 완료하기 위해 추가 TAC 조사가 필요하다는 것을 확인했습니다. 철저하고 정확한 해결을 위해 다음 단계에 대해 귀하와 긴밀히 협력하겠습니다.

Cisco는 이러한 다음 단계를 통해 귀하를 지원할 것이며, 이러한 상황을 효과적으로 해결하기 위한 명확한 지침을 제공할 것임을 확신하시기 바랍니다.

이러한 위험을 완화하기 위한 가장 중요한 단계로 업그레이드 계획 및 실행에 우선 순위를 지정해 주십시오. 아직 이 업그레이드를 예약하지 않으셨다면 즉시 예약해 주십시오.

질문이 있거나 도움이 필요한 경우 주저하지 말고 TAC 엔지니어에게 문의하십시오.

여러분의 관심과 협업에 감사드립니다.

감사합니다.

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(본문 포함)

↓ 다운로드 .eml 템플릿

TAC 2 - 결과 - IoC를 찾을 수 없음(엔지니어 확인)

사용 사례

자동화가 보안 침해 지표를 발견하지 못하고 엔지니어가 결과를 확인한 후 TAC 엔지니어가 전송했습니다.

제목

Update: TAC 검토 완료 - CVE-2026-20182에 대한 IoC를 찾을 수 없음 - 케이스 [SR #]

메시지

[고객 이름] 님, 안녕하세요?

저는 [SR 번호] 케이스에 배정된 Cisco TAC 엔지니어입니다.

SD-WAN 제어 구성 요소에서 제공한 admin-tech 파일의 예비 검사를 수행한 후 Cisco SD-WAN Security Advisories에 설명된 보안 침해 지표와 일치하는 로그 항목을 찾지 못했습니다.

- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability [1]
- Cisco Catalyst SD-WAN Manager 취약성 [2]

그러나 모든 SD-WAN 제어 구성 요소를 <insert version>으로 업그레이드해야 합니다. 업그레이드를 진행하기 위한 단계는 다음과 같습니다.

- Catalyst SD-WAN 업그레이드 시작 [3]
- Cisco SD-WAN 업그레이드 가이드[4]

Cisco는 인터넷에서 IP 주소 지정의 동적 특성과 고객 네트워크에 있는 에지 장치의 예상 IP 주소에 대한 지식이 부족하기 때문에 에지 장치의 로그를 평가할 수 없습니다. 이 단계를 수동으로 완료하려면 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability Security Advisory에 명시된 피어링 이벤트 검증 지침을 따르는 것이 좋습니다. 또한 고객은 CVE-2026-20182용 보안 권고에 설명된 대로 피어링 이벤트 검증과 관련된 추가 탐지 단계를 완료하는 것이 좋습니다.

링크

[1] Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Cisco Catalyst SD-WAN Manager 취약성 -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Catalyst SD-WAN 업그레이드 시작 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Cisco SD-WAN 업그레이드 가이드 — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

감사합니다.

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

TAC 3 - 검증 - 오버레이의 IP 소유권 확인

사용 사례

로그 분석 중에 표면화된 특정 IP 주소가 SD-WAN 오버레이 인프라의 일부인지 여부를 고객에게 질문하기 위해 TAC 엔지니어가 보냅니다.

제목

[SR #] - IP 주소 검증 필요

메시지

[고객 이름]님, 안녕하세요?

제 이름은 [Your Name]이며, 케이스에 배정된 Cisco TAC 엔지니어입니다.

SD-WAN 제어 구성 요소에서 제공한 admin-tech 파일에 대한 지속적인 분석의 일환으로, 다음 IP 주소가 SD-WAN 오버레이 인프라의 일부인지 또는 이전에 일부였는지를 검증하는 데 도움이 필요합니다.

문제의 IP 주소:

- [IP 주소 1]
- [IP 주소 2]

평가를 완료하는 데 도움이 되는 사항은 다음과 같습니다.

1. 이 IP 주소가 현재 SD-WAN 오버레이의 구성 요소(예: vManage, vSmart, vBond 또는 에지 디바이스)와 연결되어 있습니까?
2. 이전에 해제되었거나 IP가 변경되었을 수 있는 SD-WAN 제어 구성 요소에서 이 IP 주소를 사용했습니까?
3. 이 IP가 재해 복구(DR) 사이트 또는 SD-WAN 구축과 관련된 다른 인프라와 연결되어 있습니까?

귀하의 빠른 답변으로 분석을 계속하고 적절한 다음 단계를 제공할 수 있습니다.

궁금한 점이 있으시면 언제든지 문의해 주십시오.

감사합니다.

① 보내기 전에 [괄호 안의 자리 표시자]를 모두 바꿉니다.

✉ Open Outlook(본문 포함)

↓ 다운로드 .eml 템플릿

TAC 4 - 결과 - 오탐 제거됨

사용 사례

수동 검토 후 TAC 엔지니어가 보낸 결과, 자동 스캐닝으로 플래그가 지정된 초기 IoC가 오탐으로 확인되었습니다.

제목

Update: CVE-2026-20182에 대한 기술 검토 - 케이스 [케이스 번호]

메시지

고객님,

엔지니어링 팀에서 SD-WAN 제어 구성 요소에서 제공한 관리 기술 파일을 수동으로 검토하는 동안 기다려 주셔서 감사합니다.

철저한 조사 결과, 당사의 자동 스캐닝 프로세스에서 플래그된 초기 IoC(indicators of compromise)가 오탐임을 확인했습니다. 즉, 당사의 평가는 IoC가 유효하지 않다는 것입니다.

중요: 이 특정 알림은 제거되었지만 [CVE-2026-20182](#)^[1]과 관련된 취약성은 SD-WAN 패브릭의 장기적인 보안 및 무결성을 보장하려면 소프트웨어 업그레이드가 필요합니다.

업그레이드를 아직 완료하지 않은 경우: 가능한 한 빨리 SD-WAN 제어 구성 요소의 전체 업그레이드에 우선 순위를 지정해 주십시오. 업그레이드는 이러한 취약성을 효과적으로 해결할 수 있는 유일한 방법입니다. 자세한 지침은 [Cisco SD-WAN 업그레이드 가이드](#)^[2]를 참조하십시오.

업그레이드를 이미 완료한 경우: 이 확인 결과는 오탐으로 확인되었으며 귀하는 소프트웨어 교정을 이미 수행했으므로 추가 조치가 필요하지 않습니다. 이 케이스가 해결되었다고 간주하고 표준 마감 절차를 진행할 수 있습니다.

인프라 보안의 우선 순위를 정하는 데 성실히 임해 주셔서 감사합니다. 더 궁금한 점이 있거나 추가 지원이 필요한 경우 언제든지 문의해 주시기 바랍니다.

감사합니다.

Cisco TAC(Technical Assistance Center)

링크:

[1] [공식 보안 자문](#)

[2] [Cisco SD-WAN 업그레이드 가이드](#)

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

TAC 5 - 중요 - IoC 식별, 검토 통화 일정 예약

사용 사례

잠재적 IoC(Indicators of Compromise)가 확인되었고 조사 결과와 다음 단계를 논의하기 위해 긴급한 고객 통화가 필요한 경우 TAC 엔지니어가 보냅니다.

제목

긴급: CVE-2026-20182에 대한 분석 결과 - 보안 침해 지표 파악

메시지

고객님,

SD-WAN 제어 구성 요소에 대해 제공된 관리 기술 파일을 분석하는 동안 기다려 주셔서 감사합니다.

기술 검토를 마친 후 CVE-2026-20182와 관련된 잠재적 IoC(Indicators of Compromise, 보안 침해 지표)를 발견했습니다.

이러한 조사 결과의 특성을 고려할 때 기술 세부 사항 및 권장되는 다음 단계에 대해 가능한 한 빨리 논의하는 것이 중요합니다. 구체적인 조사 결과를 검토하고 적절한 치료 방법을 논의하기 위해 귀사 팀과 통화 일정을 잡고자 합니다.

다음 단계:

- **미팅 예약:** 이러한 결과를 검토하기 위해 4-8시간 내에 간단한 통화가 가능한지 여부를 알려 주십시오.
- **SDWAN 제어 구성 요소 업그레이드:** SDWAN 관리자, 컨트롤러 및 검증기를 가능한 빨리 고정 릴리스로 업그레이드하십시오.

Cisco의 기본 목표는 고객의 환경을 보호하고 잠재적 위험을 완화하는 데 도움이 되는 것입니다. 이 문제에 대해 조속히 처리해 주셔서 감사드리며 귀사와의 협조가 이루어지기를 기대합니다.

감사합니다.

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(본문 포함)

↓ 다운로드 .eml 템플릿

TAC 6 - 결과 - 중복 IoC(닫기 및 리디렉션)

사용 사례

IoC 분석을 통해 동일한 고객/환경에 대한 이전 SR과 일치하는 결과가 확인되면 TAC 엔지니어가 보냅니다. 현재 케이스는 종료되고 고객은 이미 리미디에이션 지침이 제공된 원래 SR로 리디렉션됩니다.

제목

Update: CVE-2026-20182에 대한 기술 검토 - 케이스 [SR #] (중복 IoC 확인됨)

메시지

고객님,

SD-WAN 제어 구성 요소에 대해 제공된 관리 기술 파일을 분석하는 동안 기다려 주셔서 감사합니다. 당사는 당사의 스캐닝 프로세스에서 플래그된 초기 IoC(Indicators of Compromise, 보안 침해 지표)가 [Original SR #]에서 이미 전달된 것과 동일하다고 판단했습니다. 앞서 설명한 대로, 최대한 빨리 환경을 보호하기 위해 [TAC Remediation Guide](#)^[2]에 요약된 두 가지 교정 경로 중 하나를 계속 진행하여 긴급 업그레이드를 수행하는 것이 좋습니다. 자세한 내용은 [CVE-2026-20182](#)^[1]의 [공식 보안](#) 권고 사항을 참조하십시오.

이제 이 케이스를 종료하도록 진행하겠습니다. 업그레이드 또는 리미디에이션과 관련하여 추가 지침 또는 기술 지원을 요청하려면 [Original SR #]를 사용하십시오.

감사합니다.

[이름]

링크:

[1] [공식 보안 자문](#)

[2] [TAC 리미디에이션 가이드](#)

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(본문 포함)

↓ 다운로드 .eml 템플릿

TAC 7 - 리미디에이션 - 옵션 후속 조치(통화 후)

사용 사례

IoC 검토 통화 후 전송되어 논의된 교정 경로를 다시 캡처합니다. 고객은 옵션 A(롤링 재시작을 통한 재구축), 옵션 B(하드 컷오버를 통한 재구축) 또는 옵션 C(전체 시스템 재구축)를 선택합니다.

제목

후속 조치: CVE-2026-20182 교정 옵션

메시지

고객님,

최근 분석에서 얻은 결과를 논의할 시간을 내주셔서 감사합니다. 이전 통화에서 설명했듯이, 환경을 보호하기 위해 다음 교정 경로 중 하나를 진행하는 것이 좋습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성

요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

다음 단계:

- 이러한 옵션에 대해 내부적으로 논의하고 어떤 경로를 선택할지 알려 주십시오. 결정을 내렸으면 실행 단계를 진행하는 데 도움이 되도록 추가 지침 또는 기술 지원을 제공할 수 있습니다.

Cisco는 이 과정 전반에 걸쳐 여러분을 지원하기 위해 최선을 다하고 있습니다. 이 옵션에 대해 문의 사항이 있으면 알려주시기 바랍니다.

감사합니다.

Cisco TAC(Technical Assistance Center)

참고: 옵션 1은 업그레이드였습니다. 이 업그레이드로 간주된 시나리오가 이미 수행되었습니다.

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

TAC 8 - 교정 - 손상된 패브릭에 대한 업데이트된 옵션(옵션 2 후속 조치)

사용 사례

SD-WAN 패브릭이 손상되어 이전에 옵션 2를 추구했으며 해당 패브릭이 위협 행위자의 지속성 위협에 노출된 것으로 판단되는 고객에게 알립니다. 손상된 패브릭을 재구축하고 백업/기존 configDB에 의존하지 않은 고객은 위험성이 있는 것으로 간주되지 않으며 이 커뮤니케이션을 수신하지 않습니다. 이 커뮤니케이션은 TBD로 전송됩니다.

제목

긴급 조치 필요: SD-WAN 인프라 중요 취약성 교정

메시지

고객님,

[SR#] 및 이전에 전달한 보안 권고 사항에서 설명한 대로 SD-WAN 패브릭의 교정을 위해 중요한 업데이트를 제공합니다. 이 업데이트는 제공된 로그에 IOC(Indicators of Compromise)의 증거가 나타난 해당 패브릭에만 적용됩니다.

이전에 소프트웨어 업그레이드, 컨트롤러 재구축, SSH 키 순환을 통합하는 옵션 2를 기반으로 교정 계획을 선택했지만, 위협 환경에 대한 분석은 계속 발전하고 있습니다. 이러한 취약성 악용에 대한 새로운 기술적 통찰력은 지속성의 위험을 줄이고 인증서 신뢰 체인의 무결성을 보장하는 데 도움이 되는 추가 조치가 강력하게 요구된다는 것을 나타냅니다.

필요한 조치:

루트 인증서의 추가 회전을 포함하여 보다 포괄적인 방어를 제공하기 위해 권장 교정 전략을 업데이트했습니다.

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다.

Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위험 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. TAC(Technical Assistance Center)에 SR(Service Request)을 열어 추가 기술 설명이 필요한 경우 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

TAC 17 - 역조사 결과 - 이전에는 IoC가 없었고, 이제 IoC가 식별됨(CVE-2026-20182)

사용 사례

이전에 IoC(Indicators of Compromise)가 발견되지 않았지만, 이후 관리 기술 로그의 후속 내부 검토가 CVE-2026-20182와 관련된 IoC를 식별한 고객에게 전송되었습니다. 수정된 결과를 전달하고 세 가지 교정 옵션(옵션 A, B 또는 C)을 제공합니다.

제목

중요 업데이트: CVE-2026-20182에 대한 IoC 평가 수정 - Indicators of Compromise Now Identified - SR [SR#]

메시지

고객님,

서비스 요청 [SR#]에 따라 CVE-2026-20182과 관련하여 Cisco TAC(Technical Assistance Center)에 지속적으로 협조해 주셔서 감사합니다.

이전 서신에서는 SD-WAN 제어 구성 요소에서 제공된 관리 기술 파일을 분석한 결과 이 권고와 관련된 IoC(Indicators of Compromise)가 식별되지 않았다고 조언했습니다. Cisco는 고객의 보안에 대한 지속적인 노력의 일환으로, 그 후 귀사의 패브릭과 관련된 추가 관리 기술 로그 데이터에 대한 정기적인 내

부 검토를 수행했습니다.

이 후속 검토에서는 초기 평가 중에 드러나지 않은 IoC(Indicators of Compromise, 보안 침해 지표)를 확인했습니다. 저희는 현재 여러분과 함께 이러한 결과를 해결하기 위해 노력하고 있습니다. 이러한 IoC는 조직의 패브릭 내에서 위협 요소 제거 작업을 수행할 수 있는 의심스러운 활동을 나타냅니다.

Cisco는 이러한 조치가 귀하에게 이전에 전달되었던 결과를 수정하는 것임을 인식하고 있으며, 적절한 조치를 취할 수 있도록 귀하의 환경을 명확하고 정확하게 파악하고자 합니다.

필요한 조치:

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다.

Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위협 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술 설명이 필요한 경우,

이 이메일 또는 기존 SR(Service Request)을 통해 Technical Assistance Center(TAC)에 회신하여 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

CloudOps 1 - 사전 대응적 - 클라우드 스캔에서 탐지된 IoC, 검증을 위해 필요한 관리 기술

사용 사례

클라우드 호스팅 SD-WAN 패브릭의 Cisco CloudOps 보안 스캔에서 잠재적 IoC(Indicators of Compromise)가 발견되었을 때 사전 대응적으로 전송됩니다. 고객을 대신하여 SR을 열고, 전체 로그 분석을 통해 결과를 검증할 수 있도록 admin-tech 파일을 첨부하도록 고객에게 요청합니다.

제목

필요한 조치: 보안 검사 결과를 검증하는 데 필요한 Admin-Tech 파일 - SR [SR#]

메시지

고객님,

Cisco 오퍼의 무결성을 보호하고 모니터링하기 위한 지속적인 노력의 일환으로 Cisco는 최근 일부 클라우드 호스팅 SD-WAN 패브릭에 대한 보안 검사를 완료했습니다. 이 조치는 보고된 보안 문제에 대한 응답으로 수행되었습니다. 스캔을 통해 조직의 패브릭에서 의심스러운 활동이 발견되었으며 이에 대한 추가 검토가 필요합니다.

이 결과를 검증하고 조사를 완료할 수 있도록 귀하를 대신하여 개설된 이 SR(Service Request)에 admin-tech 파일을 첨부하기 위해 귀하의 도움을 요청합니다.

전체 분석을 활성화하려면 모든 SD-WAN 제어 구성 요소에서 admin-tech 파일을 수집하고 업로드하십시오. 다음 파일을 생성할 때 "Logs" 및 "Tech"를 모두 선택해야 합니다.

- vSmarts(컨트롤러): 동시에 수집하지 말고 한 번에 하나씩 수집하십시오.
- vBonds(유효성 검사기): 모든 노드에서 수집합니다.
- 관리자(vManage): 클러스터의 모든 노드(활성 및 대기 DR)에서 수집합니다.

관리 기술 파일을 생성하고 안전하게 전송하는 방법에 대한 자세한 단계별 지침은 다음 가이드를 참조하십시오. [Cisco SD-WAN 관리 기술 수집 가이드](#)^[1].

요청한 파일을 받으면, Cisco 팀은 이를 분석하여 관찰된 활동이 진정한 보안 침해 지표를 나타내는지 확인하고 적절한 다음 단계를 알려드립니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술적 설명이 필요한 경우 본 서비스 요청(SR)에 회신하여 알려주십시오.

감사합니다.

Cisco

링크:

[1] [Cisco SD-WAN 관리 기술 수집 가이드](#)

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

옵션 A, B 또는 C를 아직 완료하지 않은 이전에 영향을 받은 고객을 위한 WAVE 2A 이메일. (옵션 1과 2를 다시 수행해야 함)

PSIRT2a에 대한 IOC 없음을 위한 TAC 9 템플릿/재구축함(이전 영향)

사용 사례

SD-WAN 로그에 PSIRT2a 권고와 관련된 IoC(Indicators of Compromise)가 표시되지 않았고 이전에 패브릭을 재구축한 고객에게 전송된 세 가지 옵션(옵션 2 후속 조치)을 통해 업데이트된 교정 지침을 제공합니다.

제목

긴급 조치 필요: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)의 최근 SD-WAN PSIRT 권고와 관련하여 Cisco TAC(Technical Assistance Center)에 연락해 주셔서 감사합니다.

SD-WAN 패브릭에서 제공된 로그 및 정보를 검토한 후, 본 분석에 따르면 2026년 6월 5일 SD-WAN 취약성 권고와 관련된 IOC(Indicators of Compromise)가 식별되지 않았습니다. 또한, 이전 권고와 관련된 문제 개선 노력의 일환으로 귀하의 환경을 재구축했다는 사실도 알고 있습니다.

이러한 취약성과 관련하여 새로 확인된 통찰력을 고려하여 SD-WAN 패브릭에 대한 권장 교정 지침에 관한 중요한 업데이트를 공유하고자 합니다.

[SR#] 및 이전에 전달한 보안 권고 사항에서 설명한 대로 SD-WAN 패브릭의 교정을 위해 중요한 업데이트를 제공합니다.

이전에 소프트웨어 업그레이드, 컨트롤러 재구축, SSH 키 순환을 통합하는 옵션 2를 기반으로 교정 계획을 선택했지만, 위협 환경에 대한 분석은 계속 발전하고 있습니다. 이러한 취약성 악용에 대한 새로운 기술적 통찰력은 지속성의 위험을 줄이고 인증서 신뢰 체인의 무결성을 보장하는 데 도움이 되는 추가 조치가 강력하게 요구된다는 것을 나타냅니다.

필요한 조치:

루트 인증서의 추가 회전을 포함하여 보다 포괄적인 방어를 제공하기 위해 권장 교정 전략을 업데이트했습니다.

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다. Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위협 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술적 설명이 필요한 경우, 이 이메일에 회신하거나 기존 서비스 요청을 통해 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

예 PSIRT2a의 IOC에 대한 TAC 10 템플릿/재구축 완료(이전 영향)

사용 사례

SD-WAN 로그에 PSIRT2a 권고와 관련된 IoC(Indicators of Compromise)가 표시된 고객 및 이전에 패브릭을 재구축한 고객에게 전송됨. 세 가지 옵션(옵션 2 후속 조치)을 통해 업데이트된 교정 지침을 제공합니다.

제목

긴급 조치 필요: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)의 최근 SD-WAN PSIRT 권고와 관련하여 Cisco TAC(Technical Assistance Center)에 연락해 주셔서 감사합니다.

Cisco 팀은 SD-WAN 패브릭에서 제공된 로그를 분석한 후 2026년 6월 5일 SD-WAN 취약성 권고와 관련된 IOC(Indicators of Compromise)를 확인했습니다. 또한 이전 권고와 관련된 리미디에이션 단계의 일환으로 귀사의 환경이 이전에 재구축되었다는 사실도 알고 있습니다.

[SR#] 및 이전에 전달한 보안 권고 사항에서 설명한 대로 SD-WAN 패브릭의 교정을 위해 중요한 업데이트를 제공합니다. 이 업데이트는 제공된 로그에 IOC(Indicators of Compromise)의 증거가 나타난 해당 패브릭에만 적용됩니다.

이전에 소프트웨어 업그레이드, 컨트롤러 재구축, SSH 키 순환을 통합하는 옵션 2를 기반으로 교정 계획을 선택했지만, 위협 환경에 대한 분석은 계속 발전하고 있습니다. 이러한 취약성 악용에 대한 새로운 기술적 통찰력은 지속성의 위험을 줄이고 인증서 신뢰 체인의 무결성을 보장하는 데 도움이 되는 추가 조치가 강력하게 요구된다는 것을 나타냅니다.

필요한 조치:

루트 인증서의 추가 회전을 포함하여 보다 포괄적인 방어를 제공하기 위해 권장 교정 전략을 업데이트했습니다.

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다. Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위협 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술적 설명이 필요한 경우, 이 이메일에 회신하거나 기존 서비스 요청을 통해 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

PSIRT2a에 대한 IOC 없음을 위한 TAC 11 템플릿/재구축하지 않음(이전 영향)

사용 사례

SD-WAN 로그에 PSIRT2a 권고와 관련된 IoC(Indicators of Compromise)가 표시되지 않았고 패브릭을 재구축하지 않은 고객에게 전송됨. 세 가지 옵션(옵션 1 후속 조치)을 통해 업데이트된 교정 지침을 제공합니다.

제목

긴급 조치 필요: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)의 최근 SD-WAN PSIRT 권고와 관련하여 Cisco TAC(Technical Assistance Center)에 연락해 주셔서 감사합니다.

SD-WAN 패브릭에서 제공된 로그 및 정보를 검토한 후 2026년 6월 5일 SD-WAN 취약성 권고와 관련된 IOC(Indicators of Compromise)를 식별하지 못했습니다.

또한 이전 권고 사항에 따라 환경이 완전히 재구축되지 않은 것으로 알고 있습니다. Cisco는 잠재적인 노출을 줄이고 SD-WAN 인증서 신뢰 체인의 무결성을 강화하기 위해 아래의 업데이트된 교정 지침을 검토할 것을 권장합니다.

이를 염두에 두고, [SR#] 및 이전에 전달한 보안 권고 사항과 같이 SD-WAN 패브릭의 교정을 위한 중요한 업데이트를 제공합니다.

이전에 소프트웨어 업그레이드와 SSH 키 순환을 통합하는 옵션 1을 기반으로 교정 계획을 선택했지만, 위협 환경에 대한 분석은 계속 발전하고 있습니다. 이러한 취약성 악용에 대한 새로운 기술적 통찰력은 지속성의 위험을 줄이고 인증서 신뢰 체인의 무결성을 보장하는 데 도움이 되는 추가 조치가 강력하게 요구된다는 것을 나타냅니다.

필요한 조치:

루트 인증서의 추가 회전을 포함하여 보다 포괄적인 방어를 제공하기 위해 권장 교정 전략을 업데이트했습니다.

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다. Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위험 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술적 설명이 필요한 경우, 이 이메일에 회신하거나 기존 서비스 요청을 통해 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

예 PSIRT2a용 IOC용 TAC 12 템플릿/재구축하지 않음(이전 영향)

사용 사례

SD-WAN 로그에 PSIRT2a 권고와 관련된 IoC(Indicators of Compromise)가 표시되고 패브릭을 재구축하지 않은 고객에게 전송됨. 세 가지 옵션(옵션 1 후속 조치)을 통해 업데이트된 교정 지침을 제공합니다.

제목

긴급 조치 필요: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)의 최근 SD-WAN PSIRT 권고와 관련하여 Cisco TAC(Technical Assistance Center)에 연락해 주셔서 감사합니다.

Cisco 팀은 SD-WAN 패브릭에서 제공된 로그를 분석한 후 2026년 6월 5일 SD-WAN 취약성 권고와 관련된 IOC(Indicators of Compromise)를 확인했습니다. 또한 귀하의 환경은 이전의 권고에 따라 완전히 재구축되지 않은 것으로 알고 있습니다.

이러한 지표가 존재하고 위협 환경에 대한 이해도가 진화하고 있는 상황에서, 지속성의 위험을 줄이고 SD-WAN 인증서 신뢰 체인의 무결성을 보장하려면 아래에 설명된 업데이트된 교정 지침을 검토하고 구현하는 것이 중요합니다.

[SR#] 및 이전에 전달한 보안 권고 사항에서 설명한 대로 SD-WAN 패브릭의 교정을 위해 중요한 업데이트를 제공합니다. 이 업데이트는 제공된 로그에 IOC(Indicators of Compromise)의 증거가 나타난 해당

패브릭에만 적용됩니다.

이전에 소프트웨어 업그레이드와 SSH 키 순환을 통합하는 옵션 1을 기반으로 교정 계획을 선택했지만, 위협 환경에 대한 분석은 계속 발전하고 있습니다. 이러한 취약성 악용에 대한 새로운 기술적 통찰력은 지속성의 위험을 줄이고 인증서 신뢰 체인의 무결성을 보장하는 데 도움이 되는 추가 조치가 강력하게 요구된다는 것을 나타냅니다.

필요한 조치:

루트 인증서의 추가 회전을 포함하여 보다 포괄적인 방어를 제공하기 위해 권장 교정 전략을 업데이트했습니다.

교정을 위해 추가적인 유지 보수 작업이 필요하며, 여기에는 계획된 네트워크 다운타임이 포함될 수 있습니다. Cisco의 우선 순위가 네트워크의 보안과 무결성이라는 점을 감안하여 세 가지 고유한 교정 옵션을 개발했습니다. 아래 각 옵션은 보안 보장에 대한 운영 영향의 균형을 고려하여 제공합니다. 내부 위협 상태는 고유하므로 Cisco에서는 특정 경로를 권장할 수 없습니다.

옵션 A: 롤링 재시작을 통한 재구축. 네트워크 다운타임을 방지하여 운영 연속성의 우선 순위를 지정합니다. 전환 프로세스 중에는 위협 지속성에 대한 위험이 남아 있습니다.

설명: 컨트롤러 재구축, SSH 키 및 인증서 순환이 포함됩니다. 기존 컨트롤러 구성 요소는 vManage를 통해 마이그레이션하는 동안 연결되어 새 패브릭을 배포한 다음 디바이스가 마이그레이션되는 즉시 각각 제거됩니다.

옵션 B: 하드 컷오버로 재구축. 더 높은 수준의 보안 보증을 제공합니다. 새 컨트롤러는 이전 컨트롤러에 연결되지 않으므로 완전히 격리됩니다. 따라서 모든 디바이스는 연결을 재설정하고 경로/연결 정보를 교환해야 하므로 전체 네트워크 운영에 영향을 미칩니다. 중단 시간은 사이트 수, 교환된 접두사 수 등에 따라 달라집니다.

설명: 컨트롤러 재구축과 SSH 키 및 인증서 순환이 포함되지만, 재구축 과정에서 이전 컨트롤러 구성 요소가 새 패브릭에서 격리됩니다.

옵션 C: 전체 시스템 재구축. 가장 복잡한 접근 방식이며 재구축 과정에서 컨피그레이션 관련 불안정성의 위험이 높지만, 클린 베이스라인을 구축하여 최고 수준의 보안을 보장합니다. 이는 긴 옵션이며 템플릿 및 정책 데이터베이스를 재구축하는 데 전문성이 필요합니다.

팀이 이러한 옵션을 검토하고 위험 관리 표준에 가장 부합하는 접근 방식을 파악한 후, 이 메시지에 회신하여 알려주십시오. 선택 사항을 받으면 유지 보수 기간을 조정하고 실행에 필요한 기술적 준비를 시작합니다.

보안 네트워크 인프라 유지에 계속 관심을 가져주셔서 감사합니다. 추가 기술적 설명이 필요한 경우,

이 이메일에 회신하거나 기존 서비스 요청을 통해 알려주십시오.

감사합니다.

Cisco

Outlook에서 열기

① 아래의 .eml 다운로드를 사용합니다. 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

신규 고객을 위한 WAVE 2A 이메일(이전에는 영향 받지 않음)

IOC 없음/사용 가능한 고정 릴리스 없음을 위한 TAC 13 템플릿(WAVE 2a — Await Fix)

사용 사례

SD-WAN 로그에 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)가 표시되지 않았지만 현재 플랫폼/버전에 사용할 수 있는 고정 소프트웨어 릴리스가 없는 고객에게 전달됩니다. 고객에게 임시 강화 조치를 적용하고 고정 릴리스 알림을 기다리도록 조언합니다.

제목

Update: CVE-2026-20245에 대한 IoC 평가 완료 - 현재 사용 가능한 고정 릴리스 없음 - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)에 따라 CVE-2026-20245과 관련하여 Cisco TAC(Technical Assistance Center)에 문의해 주셔서 감사합니다.

SD-WAN 제어 구성 요소에서 제공한 admin-tech 파일에 대한 분석을 완료했습니다. 검토한 로그에서는 CVE-2026-20245과 관련된 IoC를 식별하지 못했습니다.

이 검토를 위해 Cisco에 검색 및 제공된 로그 데이터의 양은 [Cisco SD-WAN 강화 가이드](#)^[1]에 따라 사용

자 환경에 구성된 로그 보존 기간에 의해 제한될 수 있습니다.

중요 — 현재 사용 가능한 고정 소프트웨어 릴리스가 없습니다.

현재 현재 사용 중인 플랫폼 및 소프트웨어 버전에서 이 취약성을 해결할 수 있는 고정된 소프트웨어 릴리스가 없습니다. Cisco 엔지니어링은 고정 릴리스를 제공하기 위해 적극적으로 노력하고 있습니다. 고정 소프트웨어를 사용할 수 있게 되면 [공식 보안 권고](#)^[2]가 고정 릴리스 정보로 업데이트됩니다.

권장 중간 작업:

고정 릴리스를 기다리는 동안 노출을 줄이기 위해 다음과 같은 강화 방법을 구현하는 것이 좋습니다.

1. **강화 모범 사례 적용:** [Cisco SD-WAN 강화 가이드](#)^[1]의 권장 사항을 검토 및 구현하여 공격 표면을 줄입니다.
2. **Security Advisory 모니터링:** 플랫폼의 고정 [릴리스 가용성](#)에 대한 업데이트를 정기적으로 확인하십시오^[2].
3. **업그레이드 계획:** 이제 업그레이드 계획을 시작하여 고정 릴리스가 게시되면 업그레이드를 즉시 실행할 수 있도록 준비하십시오.
4. **환경 모니터링:** SD-WAN 제어 구성 요소의 비정상적인 동작 또는 예기치 않은 컨피그레이션 변경을 계속 모니터링합니다.

다음 단계:

고정 소프트웨어 릴리스가 사용 가능해지면 이 케이스를 업데이트하겠습니다. 이 시점에서 모든 SD-WAN 제어 구성 요소(Manager, Controller, Validator)를 가능한 한 빨리 고정 버전으로 업그레이드하도록 우선 순위를 지정해야 합니다.

BCS/LCS 서브스크립션이 있는 경우 Cisco NCE 또는 Delivery Manager에 문의하여 업그레이드 계획에 대한 추가 지침을 확인하십시오.

인프라 보안에 대한 여러분의 인내심과 헌신에 감사드립니다. 질문이 있거나 중간에 추가 지원이 필요한 경우 주저하지 말고 이 케이스에 응답해 주십시오.

감사합니다.

Cisco TAC(Technical Assistance Center)

링크:

[1] [Cisco SD-WAN 강화 가이드](#)

[2] [공식 보안 자문\(cisco-sa-sdwan-privesc-4uxFrzx\)](#)

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

IOC/고정 릴리스를 사용할 수 없는 TAC 14 템플릿(WAVE 2a — 지금 업그레이드)

사용 사례

SD-WAN 로그에 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)가 표시되지 않고 고정 소프트웨어 릴리스가 사용 가능한 고객에게 전송됩니다. 고객에게 업그레이드 계획 및 실행을 즉시 진행하도록 조언합니다.

제목

Update: CVE-2026-20245에 대한 IoC 평가 완료 - IoC 없음, 업그레이드 필요 - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)에 따라 CVE-2026-20245과 관련하여 Cisco TAC(Technical Assistance Center)에 문의해 주셔서 감사합니다.

SD-WAN 제어 구성 요소에서 제공한 admin-tech 파일에 대한 분석을 완료했습니다. 검토한 로그에서는 CVE-2026-20245과 관련된 IoC를 식별하지 못했습니다.

이 검토를 위해 Cisco에 검색 및 제공된 로그 데이터의 양은 [Cisco SD-WAN 강화 가이드](#)^[1]에 따라 사용자 환경에 구성된 로그 보존 기간에 의해 제한될 수 있습니다.

중요 — 업그레이드 필요:

어떤 IoC도 식별되지 않았지만 SD-WAN 제어 구성 요소가 고정 소프트웨어 릴리스로 업그레이드될 때까지 기본 취약성은 그대로 유지됩니다. 이제 플랫폼에서 고정 릴리스를 사용할 수 있습니다.

이 취약성 문제를 해결하는 가장 중요한 단계로 업그레이드 계획 및 실행의 우선 순위를 지정해 주십시오. 아직 이 업그레이드를 예약하지 않으셨다면 즉시 예약해 주십시오.

다음 단계:

- 모든 SD-WAN 제어 구성 요소 업그레이드: 관리자(vManage), 컨트롤러(vSmart) 및 검증기(vBond)를 [공식 보안 권고](#)^[2]에 나열된 고정 소프트웨어 버전으로 업그레이드합니다.
- 업그레이드 리소스: 자세한 업그레이드 지침은 다음 Cisco 공식 문서를 참조하십시오.

- [Catalyst SD-WAN 업그레이드 시작](#)^[3]
- [Cisco SD-WAN 업그레이드 가이드](#)^[4]

3. **케이스 마감:** 환경 전반에서 소프트웨어 업그레이드를 성공적으로 완료한 후에는 이 케이스가 해결된 것으로 간주하고 표준 마감 절차를 진행할 수 있습니다.

BCS/LCS 서브스크립션이 있는 경우 Cisco NCE 또는 Delivery Manager에 문의하여 업그레이드 프로세스에 대한 추가 지침을 확인하십시오.

우리는 당신의 사례를 계속 모니터링 할 것입니다. 10일(영업일 기준) 이내에 회신이 없을 경우 추가 지원이 필요하지 않다고 가정하고 정상적인 TAC 케이스 마감 절차를 진행합니다.

감사합니다.

Cisco TAC(Technical Assistance Center)

링크:

[1] [Cisco SD-WAN 강화 가이드](#)

[2] [공식 보안 자문\(cisco-sa-sdwan-privesc-4uxFrzx\)](#)

[3] [Catalyst SD-WAN 업그레이드 시작](#)

[4] [Cisco SD-WAN 업그레이드 가이드](#)

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

IOC 식별/고정 릴리스용 TAC 15 템플릿 사용 가능(WAVE 2a — 긴급 업그레이드)

사용 사례

SD-WAN 로그에 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)가 표시되고 고정 소프트웨어 릴리스가 사용 가능한 고객에게 전송됩니다. 고객에게 긴급하게 업그레이드하고 조사 결과 및 교정에 대해 논의하기 위한 검토 통화를 예약하라고 조언합니다.

제목

긴급: CVE-2026-20245에 대해 식별된 IoC - 즉시 업그레이드 필요 - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)에 따라 CVE-2026-20245과 관련하여 Cisco TAC(Technical Assistance Center)에 문의해 주셔서 감사합니다.

SD-WAN 제어 구성 요소에서 제공된 관리 기술 파일을 분석한 결과, Cisco 팀은 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)를 확인했습니다.

이러한 조사 결과의 특성을 고려할 때 기술 세부 사항 및 권장되는 다음 단계에 대해 가능한 한 빨리 논의하는 것이 중요합니다. 구체적인 조사 결과를 검토하고 적절한 치료 경로를 논의하기 위해 귀사 팀과 통화 일정을 잡고자 합니다.

즉각적인 조치 필요:

1. **즉시 SD-WAN 제어 구성 요소 업그레이드:** 플랫폼에서 고정 소프트웨어 릴리스를 사용할 수 있습니다. 관리자(vManage), 컨트롤러(vSmart), 유효성 검사기(vBond)를 [공식 보안 권고](#)^[1]에 나열된 고정 소프트웨어 버전으로 가능한 빨리 업그레이드하십시오. 업그레이드로 인해 취약성이 즉시 종료됩니다.
2. **검토 통화 예약:** IoC 조사 결과를 검토하고 권장 치료 옵션에 대해 논의할 수 있도록 다음 시간(예: 4-8시간) 내에 간단한 통화 가능 여부를 알려 주십시오.
3. **강화 모범 사례 적용:** 교정이 계획되는 동안 공격 표면을 줄이기 위해 [Cisco SD-WAN Hardening Guide](#)^[2]의 권장 사항을 검토하고 구현합니다.

업그레이드 리소스:

- [Catalyst SD-WAN 업그레이드 시작](#)^[3]
- [Cisco SD-WAN 업그레이드 가이드](#)^[4]

중요: 업그레이드 후에는 식별된 보안 침해의 심각도에 따라 추가 교정 단계(예: 컨트롤러 재구축 및 인증서 회전)가 권장될 수 있습니다. 이러한 내용은 검토 통화 중에 설명됩니다.

자세한 교정 옵션은 [TAC Remediation Guide](#)^[5]를 참조하십시오.

Cisco의 기본 목표는 고객의 환경을 보호하고 잠재적 위험을 완화하는 데 도움이 되는 것입니다. 이 문제에 대해 조속히 처리해 주셔서 감사드리며 귀사와의 협조가 이루어지기를 기대합니다.

감사합니다.

Cisco TAC(Technical Assistance Center)

링크:

[1] [공식 보안 자문\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Cisco SD-WAN 강화 가이드](#)

[3] [Catalyst SD-WAN 업그레이드 시작](#)

[4] [Cisco SD-WAN 업그레이드 가이드](#)

[5] [TAC 개선 가이드](#)

Outlook에서 열기

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

IOC용 TAC 16 템플릿 식별/사용 가능한 고정 릴리스 없음(WAVE 2a — 고정 및 대기 수정)

사용 사례

SD-WAN 로그에 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)가 표시되었지만 현재 플랫폼/버전에 사용할 수 있는 고정 소프트웨어 릴리스가 없는 고객에게 전달됩니다. 즉각적인 강화 권고, 검토 통화 예약, 그리고 고객에게 완전한 해결을 위해 고정 릴리스를 기다려야 함을 알립니다.

제목

긴급: CVE-2026-20245에 대해 식별된 IoC - 현재 사용 가능한 고정 릴리스 없음 - SR [SR#]

메시지

고객님,

Service Request [SR#](서비스 요청)에 따라 CVE-2026-20245과 관련하여 Cisco TAC(Technical Assistance Center)에 문의해 주셔서 감사합니다.

SD-WAN 제어 구성 요소에서 제공된 관리 기술 파일을 분석한 결과, Cisco 팀은 CVE-2026-20245과 관련된 IoC(Indicators of Compromise)를 확인했습니다.

이러한 발견의 심각성을 고려할 때 기술적 세부 사항을 논의하고 임시 조치를 권장하는 것이 매우 중요합니다. 구체적인 조사 결과를 검토하기 위해 귀사와 통화 일정을 잡고자 합니다.

중요 — 현재 사용 가능한 고정 소프트웨어 릴리스가 없습니다.

현재 현재 사용 중인 플랫폼 및 소프트웨어 버전에서 이 취약성을 완전히 해결할 수 있는 고정 소프트웨어 릴리스가 없습니다. Cisco 엔지니어링은 고정 릴리스를 제공하기 위해 적극적으로 노력하고

있습니다. 고정 소프트웨어를 사용할 수 있게 되면 [공식 보안 권고](#)^[1]이 고정 릴리스 정보로 업데이트됩니다.

즉각적인 조치 필요:

1. **검토 통화 예약:** IoC 조사 결과를 검토하고 임시 억제 조치에 대해 논의하기 위해 4-8시간 내에 간단한 통화를 할 수 있는지 알려주십시오.
2. **강화 모범 사례를 즉시 적용:** 고정 릴리스를 기다리는 동안 공격 표면을 줄이려면 [Cisco SD-WAN Hardening Guide](#)^[2]의 권장 사항을 검토하고 구현하십시오.
3. **향상된 모니터링:** SD-WAN 제어 구성 요소의 비정상적인 동작, 예기치 않은 컨피그레이션 변경 또는 무단 액세스 시도를 면밀히 모니터링합니다.
4. **Security Advisory 모니터링:** 플랫폼의 고정 [릴리스 가용성에](#) 대한 업데이트를 정기적으로 확인하십시오^[1].
5. **업그레이드 계획:** 이제 업그레이드 계획을 시작하여 고정 릴리스가 게시되면 업그레이드를 즉시 실행할 수 있도록 준비하십시오.

다음 단계:

고정 소프트웨어 릴리스가 사용 가능해지면 이 케이스를 업데이트하겠습니다. 이 시점에서 모든 SD-WAN 제어 구성 요소(Manager, Controller, Validator)를 즉시 고정 버전으로 업그레이드하도록 우선 순위를 지정해야 합니다. 업그레이드 후에는 통화 중에 검토된 결과를 기반으로 추가 교정 단계(예: 컨트롤러 재구축 및 인증서 순환)에 대해 설명합니다.

고정 릴리스가 사용 가능해지면 적용되는 [교정 옵션에](#) 대한 자세한 내용은 [TAC Remediation Guide](#)^[3]를 참조하십시오.

Cisco의 기본 목표는 고객의 환경을 보호하고 잠재적 위험을 완화하는 데 도움이 되는 것입니다. 이 문제에 대해 조속히 처리해 주셔서 감사드리며 귀사와의 협조가 이루어지기를 기대합니다.

감사합니다.

Cisco TAC(Technical Assistance Center)

링크:

[1] [공식 보안 자문\(cisco-sa-sdwan-privesc-4uxFrDzx\)](#)

[2] [Cisco SD-WAN 강화 가이드](#)

[3] [TAC 리미디에이션 가이드](#)

① 보내기 전에 모든 [괄호 안의 자리 표시자]를 바꿉니다.

✉ Open Outlook(제목 전용)

↓ 다운로드 .eml 템플릿

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.