

Catalyst SD-WAN 보안 권고 - 2026년 9월

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[리미디에이션 워크플로 개요](#)

[1단계: 모든 관리자에서 Admin-Tech 파일 수집](#)

[대체 방법: 수동 확인\(Admin-Tech를 수집할 수 없는 경우에만\)](#)

[2단계: 고정 소프트웨어 버전으로 업그레이드](#)

[3단계: TAC 케이스 열기 및 스캐닝을 위한 관리 기술 파일 업로드](#)

[4단계: 보안 침해가 확인된 경우 — TAC 지침](#)

[고정 소프트웨어 버전](#)

[부록: 수동 확인 단계\(Admin-Tech 수집이 불가능한 경우에만\)](#)

[보안 침해 지표를 식별하는 방법](#)

[확인 1: 서비스 프록시 액세스 로그 감사](#)

[확인 2: 관리자 서버 로그 감사](#)

[자주 묻는 질문\(FAQ\)](#)

소개

이 문서에서는 PSIRT 자문 날짜 2026년 9월 30일에 따라 중요한 SD-WAN 보안 취약성을 식별하고 수정하는 단계를 설명합니다. Cisco에서는 이 문제를 해결하기 위해 고정 소프트웨어 릴리스로 업그레이드할 것을 적극 권장합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst SD-WAN 아키텍처 및 제어 구성 요소(관리자, 컨트롤러 및 검증기)
- 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 디바

이스는 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.

이 권고는 다음 링크에서 사용할 수 있습니다.

- [Cisco Catalyst SD-WAN Manager API 인증 우회 취약성](#)(CVE-2026-76504, CWE-177). 보안 영향 등급: Critical(CVSS Base Score 9.8).

이 결함은 이 PSIRT 권고에 의해 해결됩니다.

- Cisco 버그 ID [CSCww79570](#)

이 권고는 Cisco Catalyst SD-WAN Manager(vManage)에 적용됩니다.

리미디에이션 워크플로 개요



참고: 첫 번째 고정 릴리스보다 이전 릴리스를 실행하는 모든 SD-WAN 관리자(vManage)는 취약하며 즉시 업그레이드가 필요합니다. 그러나 모든 Catalyst Manager가 보안 침해의 증거를 보이는 것은 아닙니다.

필요한 조치: 모든 Catalyst SD-WAN Manager에서 admin-techs를 수집하고, 모든 를 고정 릴리스로 업그레이드하며, Cisco TAC 케이스를 열어 TAC에서 admin-techs의 보안 침해 지표를 스캔할 수 있습니다.

TAC는 다음과 같은 경우에 사용할 수 있습니다.

- 보안 침해 지표를 제공하는 관리자 기술 검색
 - 업그레이드 중 문제가 발생할 경우 업그레이드 지원 제공
 - IoC(Indicators of Compromise: 보안침해 지표)가 확인된 경우 추가적인 치료를 안내합니다.
1. Collect Admin-Techs - 업그레이드 전에 클러스터의 모든 노드 및 재해 복구(DR) 구축을 포함한 모든 Catalyst SD-WAN Manager에서 admin-tech를 실행하여 진단 데이터가 손실되지 않도록 합니다. Log and Tech(로그 및 기술) 옵션을 선택합니다. 코어가 필요하지 않습니다.
 2. 고정 릴리스로 업그레이드 - 모든 관리자(vManage)를 고정 소프트웨어 버전 표에 나열된 고정 [소프트웨어 버전으로](#) 업그레이드합니다.
-



참고: 업그레이드하기 전에 TAC 스캔 결과를 기다리지 마십시오. 고정 릴리스로 업그

레이드하는 것이 가장 우선순위가 높으며 취약성이 종료됩니다. 3단계의 TAC 검사는 업그레이드 후 추가 조치가 필요한지 여부를 결정합니다.

3. TAC 케이스를 열고 Admin-Techs를 업로드하여 IOC(Indicators of Compromise)를 검색합니다 - Cisco TAC 케이스를 열고 1단계에서 수집된 모든 admin-tech 로그 번들을 업로드합니다. TAC는 admin-techs에서 IOC를 검색합니다.
 4. 보안 침해가 확인된 경우 TAC 지침 사용 - TAC에서 사용자 환경의 보안 침해 지표를 확인한 경우 TAC에서 제공하는 모든 교정 지침을 완료합니다. IoC(Indicators of Compromise, 보안 침해 지표)가 발견되지 않으면 업그레이드 이후 추가 조치가 필요하지 않습니다.
-

1단계: 모든 관리자에서 Admin-Tech 파일 수집

필수: 업그레이드 전에 모든 관리자(vManage)로부터 admin-tech 파일을 수집하여 진단 데이터가 손실되지 않도록 합니다. 이러한 파일은 3단계에서 TAC에서 사용자 환경의 보안 침해 지표를 검사하는 데 사용됩니다.

컬렉션:



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

1. 모든 관리자(vManage)에서 admin-tech를 실행합니다.
2. 관리자가 클러스터로 실행되는 경우 모든 클러스터 멤버에 대해 admin-tech를 실행합니다.
3. 재해 복구(DR) 구축이 있는 경우 기본 사이트와 DR 사이트의 모든 관리자에서 admin-tech를 실행합니다.

[SD-WAN 환경에서 관리 기술 수집 및 TAC 케이스에 업로드](#)



참고: TAC에서는 이러한 파일을 분석하여 여러분의 환경을 평가하고 적절한 교정 경로를 안내합니다.

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

admin-tech 파일을 공유할 수 없는 경우 수동 확인 단계를 사용할 수 있습니다. 이러한 단계는 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: 고정 소프트웨어 버전으로 업그레이드

1단계에서 admin-techs를 수집한 후 모든 관리자(vManage)를 고정 소프트웨어 버전으로 업그레이드합니다.



중요: 업그레이드하기 전에 TAC 스캔 결과를 기다리지 마십시오. 고정 릴리스로 업그레이드하는 것이 가장 우선순위가 높으며 취약성이 종료됩니다. 3단계의 TAC 검사는 업그레이드 후 추가 작업이 필요한지 여부를 결정합니다.

이 문서의 [Fixed Software Versions\(고정 소프트웨어 버전\)](#) 테이블에서 적절한 버전을 선택합니다.



경고: 업그레이드는 현재 주요 릴리스 내에 있어야 합니다. 명시적인 TAC 지침 없이 더 높은 주요 릴리스로 업그레이드하지 마십시오.

[vManage GUI 또는 CLI를 사용하여 SD-WAN 컨트롤러 업그레이드](#)



참고: 업그레이드 중에 문제가 발생하면 업그레이드 지원을 위해 TAC 케이스를 여십시오.

3단계: TAC 케이스 열기 및 스캐닝을 위한 관리 기술 파일 업로드

2단계에서 업그레이드한 후 Cisco TAC 지원 사례를 열고 1단계에서 수집한 관리 기술 파일을 업로드합니다. TAC는 관리 기술에서 보안 침해 지표를 검사합니다.

필요한 작업:

1. 제목에 CVE-ID "CVE-2026-76504"가 포함된 심각도 3 TAC 케이스를 열어 스캐닝 프로세스를 시작합니다.
2. 1단계에서 수집된 모든 admin-tech 로그 번들(클러스터 및 DR 노드를 포함한 모든 관리자)을 업로드합니다.
3. TAC에서 스캔을 완료하고 결과를 전달할 때까지 기다립니다.



참고: TAC는 admin-tech 파일을 분석하고 스캔 결과를 전달합니다. IoC(Indicators of Compromise, 보안 침해 지표)가 발견되지 않으면 업그레이드 이후 추가 조치가 필요하지 않습니다.

4단계: 보안 침해가 확인된 경우 — TAC 지침

TAC에서 해당 환경의 IoC(Indicators of Compromise)를 찾아내면 TAC에서 구체적인 리미디에이션 지침을 제공합니다. TAC에서 제공하는 모든 지침을 완료합니다.

IoC(Indicators of Compromise, 보안 침해 지표)가 식별되지 않은 경우 2단계에서 완료한 업그레이드로 충분하며 추가 교정이 필요하지 않습니다.

고정 소프트웨어 버전

이러한 소프트웨어 릴리스에는 이 취약성에 대한 수정 사항이 포함되어 있습니다. 현재 릴리스 교육 과정의 첫 번째 고정 릴리스로 업그레이드하십시오.

Cisco Catalyst SD-WAN Software 릴리스	첫 번째 고정 릴리스	사용 가능한 소프트웨어
20.9 ¹ 이전	고정 릴리스로 마이그레이션합니다.	
20.9	20.9.10.1	vManage용 20.9.10.1 업그레이드 이미지
20.12	20.12.8.2	vManage용 20.12.8.2 업그레이드 이미지
20.15	20.15.6.1	vManage용 20.15.6.1 업그레이드 이미지
20.18	20.18.4.1	vManage용 20.18.4.1 업그레이드 이미지
26.1	26.1.2.1	vManage용 26.1.2.1 업그레이드 이미지
26.2	26.2.1	vManage용 26.2.1 업그레이드 이미지

¹ 이 릴리스는 소프트웨어 유지 관리가 종료되었습니다. Cisco는 고객에게 지원되는 릴리스로 업그레이드할 것을 적극 권장합니다.

Cisco PSIRT(Product Security Incident Response Team)는 권고에 문서화된 영향과 고정 릴리스 정보만 검증합니다.



참고: Cisco는 클라우드 기반인 Cisco SD-WAN Cloud(Cisco Managed) Release 20.15.605에서도 이러한 취약성을 해결했습니다. 사용자 작업은 필요하지 않습니다. 고객은 서비스 GUI의 Help(도움말) 기능을 사용하여 현재 교정 상태 또는 소프트웨어 버전을 확인할 수 있습니다.

중요 참조:

- [업그레이드 매트릭스](#)
 - [컨트롤러 호환성 매트릭스](#)
-

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



참고: Admin-tech 수집이 기본 설정 및 권장 방법입니다. 절대적으로 관리 기술 파일을 수집하고 공유할 수 없는 경우에만 수동 확인을 사용하십시오. admin-tech 파일을 수집할 수 없는 경우 다음 수동 단계를 사용하여 TAC에 대한 예비 지표를 수집합니다.



참고:

- 이 단계에서는 예비 데이터만 제공합니다
 - 정확한 평가를 위해 관리 기술 수집이 매우 선호됨
 - 조사 결과를 문서화하고 지원 사례에서 TAC와 공유하십시오.
 - TAC에서 공식적인 평가 결정
-

요건: 이러한 단계는 모든 클러스터 멤버 및 재해 복구(DR) 사이트의 모든 관리자를 포함하여 모든 관리자(vManage)에서 수행해야 합니다. vshell에서 로그 파일(Manager CLI에서 vshell)에 액세스하고 현재 및 회전된 로그 파일을 모두 검토합니다.

보안 침해 지표를 식별하는 방법

이 자문에는 두 가지 보안 침해 지표가 있습니다. 둘 다 알 수 없거나 권한이 없는 IP 주소에서 요청 문자가 인코딩된 j_security_check(예: /%6a_security_check)에 대한 항목과 관련됩니다.



중요: 이 섹션의 예에서는 요청에서 인코딩된 문자 j로 %6a를 사용하는 것을 보여줍니다. 이는 예시일 뿐이며, 취약점은 요청에서 인코딩된 임의의 한 문자를 사용할 수 있도록 허용합니다.



참고: 인터넷에 노출되어 있고 포트가 인터넷에 노출되어 있는 Cisco Catalyst SD-WAN Manager 시스템은 보안 침해에 노출될 위험이 있습니다. 경우에 따라 이러한 보안 침해 지표는 표준 작업 중에 발생할 수 있습니다. 따라서 오탐을 식별하고 방지하기 위해 정상 네트워크 상태를 평가해야 합니다.

표시기	로그 파일	의미	확인
인코딩된 j_security_check 요청 수신	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	클라이언트가 이 유형의 요청을 관리자에게 보냈습니다.	확인 1
viptela-reserved-* 사용자에 대해 처리된 인코딩된 j_security_check 요청	/var/log/nms/vmanage-server.log*	관리자가 viptela-reserved-* 사용자(예약된 시스템 서비스 계정)에 대해 이 유형의 요청을 처리했습니다.	확인 2

확인 1: 서비스 프록시 액세스 로그 감사

다음 예에 표시된 대로 알 수 없거나 권한이 없는 IP 주소에서 j_security_check와 관련된 항목에 대해 /var/log/nms/containers/service_proxy/serviceproxy-access.log에 있는 serviceproxy-access.log 파일을 감사합니다.

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

vManage 시스템의 특정 로그 파일은 루트 액세스에서 제한되며 고객이 직접 액세스할 수 없습니다. 이러한 로그를 검토하려면 고객이 admin-tech 파일을 생성해야 합니다.

TAC용 결과 및 문서 해석

해당 항목이 없는 경우:

- 이 관리자의 이 로그에서 발견된 보안 침해 지표가 없습니다.
- 이 결과를 TAC 케이스에 문서화합니다.
- 확인 2를 계속한 다음 나머지 관리자에 대해 두 가지 확인을 반복합니다

해당 항목이 있는 경우:

- 표시된 각 소스 IP 주소를 주의 깊게 검토합니다.
- 알 수 없거나 권한이 없는 IP 주소에서 항목을 찾습니다. 소스 IP가 환경에서 인증된 활동(예: 실행하는 취약성 검사 또는 침투 테스트)에 속하는지 확인합니다.
- 소스 IP를 합법적인 것으로 식별할 수 없는 경우, 이는 잠재적인 보안 침해 지표를 나타낼 수 있습니다
- 모든 조사 결과를 문서화하고 즉시 TAC 케이스 열기
- 케이스에 로그 항목, 타임스탬프, 소스 IP 및 HTTP 상태 코드 포함
- TAC에서 공식적인 평가 결정 수행

확인 2: 관리자 서버 로그 감사

/var/log/nms/vmanage-server.log에 있는 vmanage-server.log 파일을 감사하여 알 수 없거나 권한이 없는 IP 주소에서 j_security_check와 관련된 항목, 특히 이에 표시된 대로 viptela-reserved-로 시작하는 이름을 포함하는 사용자를 위해 호출되는 항목을 확인합니다.

29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) [default] Request Store



참고: Viptela 예약 시스템 서비스 어카운트는 Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide의 Authentication, Authorization, and Accounting 섹션에 설명되어 있습니다.

TAC용 결과 및 문서 해석

해당 항목이 없는 경우:

- 이 관리자의 이 로그에서 발견된 보안 침해 지표가 없습니다.
- 이 결과를 TAC 케이스에 문서화합니다.
- 나머지 Manager에 대해 두 검증 반복

해당 항목이 있는 경우:

- 이는 잠재적 보안 침해 지표를 나타냅니다.
- 모든 조사 결과를 문서화하고 즉시 TAC 케이스 열기
- 같은 기간 동안 Verification 1 검색 결과와 함께 로그 항목 및 타임스탬프를 포함합니다.
- TAC에서 공식적인 평가 결정 수행

자주 묻는 질문(FAQ)

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

A : 모든 관리자(vManage)에서 admin-tech 파일을 수집한 다음 모든 관리자를 고정 소프트웨어 버전으로 업그레이드합니다. 업그레이드한 다음 TAC 케이스를 열고 관리 기술을 업로드하여 TAC에서 사용자의 환경에서 보안 침해 지표를 스캔할 수 있도록 합니다.

Q: 이 권고의 영향을 받는 구성 요소는 무엇입니까?

A : Cisco Catalyst SD-WAN Manager(vManage)만 영향을 받습니다.

Q: 컨트롤러, Validator 또는 에지 라우터도 업그레이드해야 하나요?

A : 아니요, 이 조언을 다루지 않습니다. 모든 Manager(vManage)를 고정 릴리스로 업그레이드하고 [Controller Compatibility Matrix](#)를 사용하여 새 Manager 릴리스가 다른 구성 요소와 호환되는지 확인합니다.

Q: 해결 방법이 있습니까?

A : 아니요. 이 취약성을 해결할 해결 방법이 없습니다. 고정 릴리스로 업그레이드합니다.

Q: 어떤 버전으로 업그레이드해야 하나요?

A : 가능한 한 빨리 현재 릴리스 트레인의 첫 번째 고정 릴리스로 업그레이드하십시오. 이 문서의 [Fixed Software Versions](#) 테이블을 참조하십시오. TAC에서 고객의 특정 환경에 적합한 버전을 확인합니다.

Q: 이전 SD-WAN 보안 권고에 대한 고정 릴리스로 이미 업그레이드했습니다. 다시 업그레이드해야 하나요?

A : 예. 현재 릴리스가 Fixed Software Versions([고정 소프트웨어 버전](#)) 테이블에 있는 열차의 첫 번째 고정 릴리스보다 [늦거나](#) 오래된 [경우](#)가 아니면 가능합니다. 이전 권고에 대한 고정 릴리스에는 반드시 이 취약성에 대한 수정 사항이 포함되어 있지 않습니다.

Q: 모든 관리자의 관리자-기술을 수집해야 하나요?

A : 예. TAC에서는 모든 클러스터 구성원 및 재해 복구(DR) 사이트의 모든 관리자를 포함하여 모든 관리자(vManage)의 관리 기술 파일을 사용하여 환경을 올바르게 평가해야 합니다.

Q: 보안 침해 지표를 직접 확인할 수 있습니까?

A : 예. admin-tech 파일을 수집할 수 없는 경우 모든 관리자에서 [수동 확인](#) 단계를 사용하고 결과를 TAC와 공유합니다. 관리자-기술 수집은 선호하는 방법으로 남아 있으며, TAC는 공식적인 평가 결과를 내립니다.

Q: TAC는 내 시스템이 손상되었는지 어떻게 판단합니까?

A : TAC는 전문 툴을 사용하여 관리 기술 파일을 분석하여 보안 침해 지표를 위한 환경을 평가합니다.

Q: 보안 침해 지표가 식별되면 어떻게 됩니까?

A : TAC에서 해당 환경에 맞는 다음 단계 및 지침을 논의하기 위해 연락합니다. Cisco는 사용자를 대신하여 교정을 수행하지 않습니다. TAC는 진행에 필요한 지침을 제공합니다.

Q: TAC에서 내 관리자-기술을 분석하기 전에 업그레이드를 시작할 수 있습니까?

A : 예. 관리 기술을 수집하고, 고정 릴리스로 업그레이드한 다음, TAC 케이스를 열어 TAC에서 관리 기술에서 보안 침해 지표를 스캔할 수 있도록 합니다.

Q: 치료 중에 다운타임이 발생합니까?

A : 구축 아키텍처 및 교정 경로에 따라 영향이 달라집니다. TAC에서는 프로세스 중 서비스 영향을 최소화하는 데 대한 지침을 제공합니다.

Q: 클라우드 호스팅 SD-WAN 오버레이가 있습니다. 업그레이드할 수 있는 옵션은 무엇입니까?

A : 클라우드 호스팅 오버레이의 경우 고객은 두 가지 옵션을 사용할 수 있습니다.

1. SSP > Overlay Details(오버레이 세부사항) > Change Windows(창 변경)로 이동하여 환경이 자동 업그레이드로 예약되었는지 확인합니다.
2. 예약된 업그레이드를 기다리지 않으려면 두 가지 옵션이 있습니다.
 - 이 문서에서 제공되는 업그레이드 가이드를 사용하여 직접 업그레이드하십시오.
 - 원하는 유지 보수 기간을 위해 대기 TAC 케이스를 엽니다. 업그레이드에 문제가 발생할 경우 TAC를 통해 지원을 받을 수 있습니다.

Q: Cisco 호스팅 오버레이입니다. SSP에 대한 액세스 규칙을 검토해야 합니까?

A : 모든 Cisco 호스팅 고객은 SSP > Overlay Details(오버레이 세부 정보) > Allow Inbound rules(인바운드 허용 규칙)에서 자신의 Allowed Inbound Rules(허용된 인바운드 규칙)를 검토하고, 사용자 측의 필요한 접두사만 허용되는지 확인하는 것이 좋습니다. 이 규칙은 관리 액세스용이며 에지 라우터에는 적용되지 않습니다.

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

A : Cisco TAC는 이 취약성과 관련된 IoC(Indicators of Compromise)를 검사하여 고객을 지원할 수 있습니다. 그러나 TAC에서는 심층 포렌식 분석이나 사고 조사를 수행하지 않습니다. 포괄적인 포렌식 작업 또는 세부적인 보안 조사를 위해 고객이 선호하는 서드파티 IR(Incident Response) 회사를 이용하는 것이 좋습니다.

Q: SD-WAN 오버레이의 취약성을 줄이기 위한 일반적인 모범 사례 또는 방법은 무엇입니까?

A : SD-WAN 오버레이의 취약점을 줄이기 위한 모범 사례 및 권장 사항은 [Cisco Catalyst SD-WAN 강화 가이드](#)를 참조하십시오.

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.