Catalyst SD-WAN Security Advisory 교정 - 2026년 2월

목차

소개

이 문서에서는 2026년 2월 25일자 PSIRT 권고 사항을 기반으로 SD-WAN의 중요한 보안 취약성을 식별하고 수정하는 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 취약성
- Cisco Catalyst SD-WAN Controller 인증 우회 취약성

이러한 결함은 다음 PSIRT 권고에 의해 해결됩니다.

- Cisco 버그 ID CSCws52722
- Cisco 버그 ID CSCws33583
- Cisco 버그 ID CSCws33584
- Cisco 버그 ID CSCws33585
- Cisco 버그 ID CSCws33586
- Cisco 버그 ID CSCws33587
- Cisco 버그 ID CSCws93470

리미디에이션 워크플로 개요

참고: 모든 SD-WAN 구축은 취약하며 즉각적인 조치가 필요합니다. 그러나 모든 시스템이 보안 침해의 증거를 보이는 것은 아닙니다.

필요한 조치: Cisco TAC 케이스를 열어 이 보안 권고 사항을 해결합니다.

TAC는 다음과 같은 경우에 사용할 수 있습니다.

- 보안 침해 지표에 대한 환경 평가
- 평가를 기반으로 적절한 교정 경로를 안내합니다.
- 보안 침해 지표가 식별된 경우 PSIRT 팀과 협력
- IoC(indicators of compromise)가 감지되지 않을 경우 업그레이드 지침 및 지원 제공

1. 관리자 기술 수집 - 모든 제어 구성 요소(vSmart, vManage, vBond)에서 관리자 기술을 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 Control Component Admin-tech 로그 번들 제

공
3. TAC 평가 - TAC에서 보안 침해 지표에 대한 환경 평가
4. 교정 실행 - TAC에서 제공하는 특정 프로세스를 완료합니다.

1단계: 모든 제어 구성 요소에서 Admin-Tech 파일 수집

필수: TAC 케이스를 열기 전에 모든 제어 구성 요소에서 admin-tech 파일을 수집합니다. 이는 TAC에서 환경을 평가하는 데 필수적입니다.

컬렉션:

참고: 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)

참고: vSmart admin-techs는 동시에 실행할 수 없습니다. 한 번에 하나씩 수집하십시오. Managers 및 Validator에 대한 Admin-techs는 임의의 순서로 수집할 수 있습니다.

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 TAC과 공유해야 하는 예비 지표를 제공합니다.

자세한 절차는 이 문서 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 모든 관리 기술 파일을 수집한 후 Cisco TAC 지원 케이스를 엽니다.

필요한 작업:

1. 비즈니스에 미치는 영향에 적합한 심각도 레벨의 TAC 케이스 열기
2. 1단계에서 수집된 모든 admin-tech 로그 번들 업로드(컨트롤러, 관리자, 검사기)
3. PSIRT 권고 사항 참조
4. TAC 평가 및 지침 대기

⚠ 주의: TAC는 시스템 상태를 확인하고 적절한 다음 단계를 권장합니다.

TAC 지침 없이 추가 단계 시도 안 함

3단계: TAC 평가

TAC는 업로드된 admin-tech 파일을 분석하고 시스템의 상태를 확인합니다.

이 시간 동안:

- 조치를 취하기 전에 TAC의 공식 평가를 기다립니다.
- TAC에서 조사 결과 및 다음 단계를 알려드립니다.

4단계: 개선 실행(TAC 유도)

TAC에서는 평가를 기반으로 적절한 교정 프로세스를 안내합니다. TAC에서 제공하는 모든 지침을 완료합니다.

경로 A: IoC(Indicators of Compromise)를 찾을 수 없음 — 업그레이드

TAC에서 보안 침해 증거가 없다고 확인될 경우, 고정 소프트웨어 버전으로 업그레이드하십시오. 이 문서의 Fixed Software Versions(고정 소프트웨어 버전) 테이블에서 적절한 버전을 선택하고 이 섹션에 연결된 업그레이드 가이드를 참조하십시오.

⚠ 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

경로 B: Indicators of Compromise Identified — PSIRT 유도

TAC에서 IoC(Indicators of Compromise, 보안 침해 지표)가 있다고 확인하면, PSIRT 팀을 참여시

켜 해당 환경에 맞는 맞춤형 교정 전략을 개발합니다. TAC 및 PSIRT에서 제공하는 모든 지침을 완료합니다.

고정 소프트웨어 버전

이러한 소프트웨어 릴리스에는 식별된 취약성에 대한 수정 사항이 포함되어 있습니다.

현재 버전에 적용	고정 버전	사용 가능한 소프트웨어
20.3, 20.6, 20.9	20.9.8.2 *	vManage, vSmart 및 vBond의 20.9.8.2 업그레이드 이미지
20.12에서 20.10, 20.11, 20.12.5 이하	20.12.5.3	vManage, vSmart 및 vBond의 20.12.5.3 업그레이드 이미지
20.12.6	20.12.6.1	vManage, vSmart 및 vBond의 20.12.6.1 업그레이드 이미지
20.13, 20.14, 20.15.x	20.15.4.2	vManage, vSmart 및 vBond의 20.15.4.2 업그레이드 이미지
20.16, 20.17, 20.18.x	20.18.2.1	vManage, vSmart 및 vBond의 20.18.2.1 업그레이드 이미지

참고: CDCS(Cisco-Hosted Cluster) 고객의 경우 20.15.405도 고정 릴리스입니다. 이는 특별히 Cisco 호스팅 클러스터 구축에 적용되며 표준 업그레이드 경로와 별도로 처리됩니다.

---

* 릴리스 20.9 이전 버전인 경우: 해당 릴리스(20.9.8.2)의 고정 소프트웨어는 2027년 2월에 제공됩니다. 더 높은 주요 릴리스(20.12, 20.15, 20.18)로 업그레이드하는 대신 현재 주요 릴리스 내에서 남아 20.9.8.2 릴리스를 기다리는 것이 좋습니다. 현재 20.9보다 낮은 버전인 경우 20.9.8.2에서 업그레이드할 때까지 기다립니다. 계속해서 TAC와 협력하고 27/27 다시 방문하여 사용 가능한 소프트웨어 링크를 확인합니다.

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 제어 구성 요소에서 수행해야 합니다.

확인 1: 인증 로그에서 인증되지 않은 SSH 로그인 확인

1단계: 유효한 vManage 시스템 IP 식별

각 vSmart 컨트롤러에 액세스하여 다음을 실행합니다.

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

출력 예:

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                    PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                              PORT    PUBLIC I
-----------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                              12346   10.1.10.1
```

2단계: 정규식 문자열 작성(vBond 및 vSmart만 해당)

1단계의 모든 시스템 IP를 OR regex 패턴으로 결합합니다.

```
system-ip1|system-ip2|...|system-ipn
```

2b단계: vManage 시스템을 위한 추가 단계

vManage 자체에서 이러한 명령을 실행하는 경우 regex에 localhost IP(127.0.0.1), local system IP,

모든 cluster IP 및 VPN 0 transport interface IP를 추가합니다.

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

로컬 vManage 시스템 IP를 찾으려면 다음을 사용합니다.

```
show control local-properties
```

VPN 0 전송 인터페이스 IP 및 클러스터 IP를 찾으려면 다음을 사용합니다.

```
show interface | tab
```

3단계: 확인 명령 실행

2단계에서 REGEX를 `regex 문자열`로 대체하여 이 명령을 실행합니다.

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

참고: 이 명령은 예기치 않은 소스의 vmanage-admin 로그인만 표시하도록 인증 로그를 필터링합니다. 합법적인 로그인은 vManage 관련 IP에서만 시작해야 합니다.

4단계: TAC용 결과 및 문서 해석

NO 출력이 표시되면

- 이 장치에서 보안 침해 지표가 탐지되지 않음
- 이 결과를 TAC 케이스에 문서화합니다.
- 나머지 컨트롤러에 대한 평가 계속

로그 라인이 인쇄되는 경우:

- 표시된 각 IP 주소를 주의 깊게 검토합니다.
- IP가 vManage 인프라와 관련이 없는지 확인합니다(클러스터 IP, 이전 시스템 IP 또는 유사).
- 소스 IP를 합법적인 것으로 식별할 수 없는 경우, 이는 잠재적인 보안 침해 지표를 나타낼 수 있습니다
- 로그 항목에는 타임스탬프 및 소스 IP 주소가 표시됩니다
- 모든 조사 결과를 문서화하고 즉시 TAC 케이스 열기
- 케이스에 로그 항목, 타임스탬프 및 소스 IP 포함
- TAC에서 공식적인 평가 결정 수행

확인 2: 컨트롤러 Syslog에서 무단 피어 연결 확인

이 명령은 컨트롤러 syslog 파일에서 모든 peer-type 및 peer-system-ip 쌍을 추출하여 검토할 목록으로 출력합니다. 의심스러운 항목은 자동으로 플래그하지 않습니다. 출력을 검사하고 각 피어 시스템 IP가 SD-WAN 인프라의 알려진 합법적인 부분인지 확인해야 합니다. 모든 컨트롤 구성 요소(컨트롤러, 관리자 및 검사기)에서 이 명령을 실행합니다.

1단계: 각 제어 구성 요소에서 명령을 실행합니다.

먼저 vshell에 액세스하여 로그 디렉토리로 이동합니다.

```
vs
cd /var/log
```

그런 다음 다음 다음 명령을 실행합니다.

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

2단계: TAC용 결과 및 문서 해석

출력에 알려진 vManage/vSmart/vBond 시스템 IP만 표시되는 경우:

- 이 검사에서 보안 침해 지표가 탐지되지 않음
- 이 결과를 TAC 케이스에 문서화합니다.
- 나머지 제어 구성 요소에 대한 평가 계속

출력에 인식할 수 없는 피어 시스템 IP가 포함된 경우:

- 표시된 각 IP 주소 및 피어 유형을 주의 깊게 검토합니다.
- IP가 알려진 SD-WAN 컨트롤 플레인 인프라와 관련이 없는지 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
- 경우에 peer-type 및 peer-system-ip 쌍과 함께 전체 명령 출력을 포함합니다
- TAC에서 공식적인 평가 결정 수행

자주 묻는 질문(FAQ)

Q: 이 보안 권고 사항을 해결하기 위한 첫 번째 단계는 무엇입니까? A : 모든 제어 구성 요소에서 admin-tech 파일을 수집하고 TAC 케이스를 열어 파일을 업로드합니다. TAC에서 환경을 평가하고 다음 단계에 대한 지침을 제공합니다.

Q. 어떤 버전으로 업그레이드해야 합니까? A. 빠른 시일 내에 가장 가까운 고정 버전으로 업그레이드하십시오.

Q: 모든 제어 구성 요소에서 admin-techs를 수집해야 합니까? A : 예. TAC에서는 환경 평가를 제대로 수행하려면 모든 컨트롤러(vSmart, 한 번에 하나씩 수집됨), 모든 관리자(vManage) 및 모든 검증자(vBond)의 관리 기술 파일이 필요합니다.

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 : TAC은 PSIRT 팀과 연락하여 귀사의 환경에 맞는 다음 단계 및 지침을 논의합니다. Cisco는 사용자를 대신하여 교정을 수행하지 않습니다. TAC는 진행에 필요한 지침을 제공합니다.

Q: 사용할 고정 소프트웨어 버전을 어떻게 알 수 있습니까?

A : 이 문서의 Fixed Software Versions 테이블을 참조하십시오. TAC에서 고객의 특정 환경에 적합한 버전을 확인합니다.

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

A : 아니요. TAC에서 평가를 완료하고 지침을 제공한 후 교정 작업을 수행합니다.

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: PSIRT 픽스는 20.15.5 릴리스와 기타 향후 릴리스에 포함되어 있습니까?

A : 예, 20.15.5 및 기타 향후 릴리스에 수정 사항이 포함되어 있습니다. 그러나 이 문서에 설명된 취약성을 완화하기 위한 업그레이드의 우선 순위를 즉시 지정해야 합니다. (기다리지 마십시오!)

Q: 보안 침해 지표가 발견되지 않을 경우 모든 컨트롤러를 업그레이드해야 합니까?

A : 예. 모든 SD-WAN 제어 구성 요소(vManage, vSmart 및 vBond)를 고정 소프트웨어 버전으로 업그레이드해야 합니다. 컨트롤러 하위 집합만 업그레이드하는 것으로는 충분하지 않습니다.

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 TAC에서 지원합니다.

Q: 에지 라우터도 업그레이드해야 합니까?

A : Cisco IOS XE 디바이스는 이 권고의 영향을 받지 않습니다.

Q: Cisco 호스팅 오버레이입니다. ACL을 수정하거나 SSP에 대한 작업을 수행해야 합니까?

A : 모든 Cisco 호스팅 고객은 SSP에 표시된 자체 Allowed Inbound Rules를 검토하고 사용자 측의 필요한 접두사만 허용하도록 확인하는 것이 좋습니다. 이 규칙은 관리 액세스용이며 에지 라우터에는 적용되지 않습니다. SSP > Overlay Details(오버레이 세부사항) > Allow Inbound rules(인바운드 허용 규칙)에서 검토하십시오. 포트 22, 830은 외부에서 클라우드 호스팅 컨트롤러로 Cisco에 의한 Day 0 프로비저닝에서 항상 기본적으로 차단되었습니다.

Q:CDCS/공유 테넌트에 있습니다. 어떤 버전으로 업그레이드할 예정입니까?

A : 현재 버전을 기준으로 공유 테넌트 또는 CDCS 클러스터는 현재 업그레이드 예정이거나 이미 고정 버전으로 업그레이드된 상태입니다. 다음은 공유 테넌트 및 CDCS 고정 릴리스입니다.

1. 조기 도입 클러스터 => 20.18.2.1(표준 릴리스와 동일)

2. 릴리스 클러스터 => 20.15.405 권장(PSIRT 픽스가 있는 CDCS 특정 버전)

CDCS 고객은 이 PSIRT를 해결하기 위해 어떤 조치도 효과적으로 취할 필요가 없습니다.

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 가이드를 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.