Catalyst SD-WAN 보안 권고 - 2026년 5월

목차

소개

이 문서에서는 2026년 5월 14일자 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 Controller 인증 우회 취약성
- Cisco Catalyst SD-WAN 취약성

이러한 결함은 다음 PSIRT 권고에 의해 해결됩니다.

- Cisco 버그 ID CSCwt50498
- Cisco 버그 ID CSCwt38739
- Cisco 버그 ID CSCwt38767
- Cisco 버그 ID CSCwt55544

리미디에이션 워크플로 개요

참고: 모든 SD-WAN 컨트롤러 및 관리자는 취약하며 모든 제어 구성 요소에 대해 즉시 업그레이드해야 합니다. 그러나 모든 컨트롤러에서 보안 침해의 증거가 나타나는 것은 아닙니다.

필요한 조치: 관리 기술을 수집하고, 고정 릴리스로 업그레이드한 다음, TAC에서 관리 기술의 보안 침해 지표를 스캔할 수 있도록 Cisco TAC 케이스를 엽니다.

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-Tech - 진단 데이터가 손실되지 않도록 업그레이드 전에 모든 제어 구성 요소(vSmart, vManage, vBond)에서 admin-tech를 실행합니다. Log and Tech 옵션을 선택합니다. 코어가 필요하지 않습니다.

   주의: vSmart admin-techs는 동시에 실행할 수 없습니다. 한 번에 하나씩 실행하십시오. 다른 모든 항목은 어떤 순서로든 수집할 수 있습니다

   ---

2. 고정 릴리스로 업그레이드 - 모든 SD-WAN 제어 구성 요소(vManage, vSmart, vBond)를 고정 소프트웨어 버전 테이블에 나열된 고정 소프트웨어 버전으로 업그레이드합니다.

참고: 업그레이드하기 전에 TAC 스캔 결과를 기다리지 마십시오. 고정 릴리스로 업그레이드하는 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 침해 지표가 확인되면 TAC 지침을 따르십시오. TAC에서 사용자 환경의 보안 침해 지표를 확인하면 TAC에서 제공하는 모든 교정 지침을 따르십시오. IoC(Indicators of Compromise, 보안 침해 지표)가 발견되지 않으면 업그레이드 이후 추가 조치가 필요하지 않습니다.

1단계: 모든 제어 구성 요소에서 Admin-Tech 파일 수집

필수: 업그레이드 전에 모든 제어 구성 요소에서 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 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: 고정 소프트웨어 버전으로 업그레이드

1단계에서 admin-techs를 수집한 후 모든 SD-WAN 제어 구성 요소(vManage, vSmart 및 vBond)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. 제목에서 "CVE-2026-20182"과 관련 PSIRT ID로 심각도 3 TAC 케이스를 열어 스캐닝 프로세스를 시작합니다.
2. 1단계에서 수집된 모든 admin-tech 로그 번들 업로드(컨트롤러, 관리자, 검사기)
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 지침을 따르십시오.

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 식별된 취약성에 대한 수정 사항이 포함되어 있습니다.

현재 버전에 적용	고정 버전	사용 가능한 소프트웨어
20.3, 20.6, 20.9	20.9.9.1	vManage, vSmart 및 vBond의 20.9.9.1 업그레이드 이미지
20.12에서 20.10, 20.11, 20.12.5 이하	20.12.5.4	vManage, vSmart 및 vBond의 20.12.5.4 업그레이드 이미지
20.12.6.x	20.12.6.2	vManage, vSmart 및 vBond의 20.12.6.2 업그레이드 이미지
20.12.7	20.12.7.1	vManage, vSmart 및 vBond의 20.12.7.1 업그레이드 이미지
20.13, 20.14, 20.15.4.3 이하 (20.15)	20.15.4.4	vManage, vSmart 및 vBond의 20.15.4.4 업그레이드 이미지
20.15.5.x	20.15.5.2	vManage, vSmart 및 vBond의 20.15.5.2 업그레이드 이미지
20.16, 20.17, 20.18.x	20.18.2.2	vManage, vSmart 및 vBond의 20.18.2.2 업그레이드 이미지

참고: SD-WAN 클라우드(이전 명칭은 Cloud Delivered Cisco Catalyst SD-WAN [CCS])를 사용하는 고객의 경우 20.15.506도 고정 릴리스입니다. 이는 특별히 Cisco 호스팅 클러스터 구축에 적용되며 표준 업그레이드 경로와 별도로 처리됩니다. 이러한 모든 고객은 이미 고정 릴리스 20.15.506으로 업그레이드되었습니다.

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 이 명령을 실행하여 vsyslog* 파일 그룹을 검색합니다.

```
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
```

messages* file glob 및 vdebug* file glob에 대해 이 작업을 반복합니다.

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

확인 3: 활성 제어 연결에서 Missing challenge-ack 확인

이 검사는 활성(또는 최근에 제거됨)으로 보고되었지만 예상되는 challenge-ack 교환이 없는 피어 세션에 대한 제어 연결 세부 출력을 검사합니다. Tx 또는 Rx 통계에서 challenge-ack 0을 표시하면서 양방향으로 hello 패킷을 교환하는 세션은 피어가 예상 챌린지 핸드셰이크를 완료하지 않았음을 나타냅니다. 이는 조사가 필요한 이상 현상입니다. 모든 컨트롤 구성 요소(컨트롤러, 관리자 및 검사기)에서 이 명령을 실행합니다.

1단계: 제어 연결 세부 정보 출력 수집

디바이스 CLI에서 다음을 실행합니다.

```
show control connections detail
show control connections-history detail
```

검사를 위해 출력을 파일(예: vdaemon.txt)에 저장합니다.

2단계: 살펴볼 내용

각 피어 레코드(REMOTE-COLOR-/SYSTEM-IP 헤더로 구분)에 대해 모든 조건이 참인 경우 레코드에 플래그를 지정합니다.

- 세션 상태가 UP 또는 TEAR_DOWN임
- Tx Statistics hello 카운터 및 Rx Statistics hello 카운터 모두 0이 아닙니다(hello는 양방향으로 흐릅니다).
- challenge-ack는 Tx Statistics 또는 Rx Statistics 블록(또는 둘 다)에서 0입니다.

일치하는 레코드의 예(누락된 challenge-ack을 강조 표시하는 <<< 화살표 참조)

```
------------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
------------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
```

```
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

위의 예에서 Tx 및 Rx `hello` 카운터는 모두 0이 아닌(활성 연결)이지만 `challenge-ack`는 양방향으로 `0`입니다.

3단계: 수동 검색 명령

저장된 vdaemon.`txt`(또는 `show control connections detail` 출력이 포함된 모든 파일)에서 후보 레코드를 빠르게 표시하려면 다음을 실행합니다.

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

반환된 각 블록은 challenge-ack이 0으로 보고된 피어 세션을 나타냅니다. 각 블록을 전체적으로 검토하여 상태가 `up` 또는 `tear_down`이고 Tx와 Rx의 hello 카운터가 0이 아닌지 확인한 다음 적중으로 처리합니다.

4단계: TAC용 결과 및 문서 해석

세 가지 조건을 모두 충족하는 레코드가 없는 경우

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

하나 이상의 레코드가 세 가지 조건을 모두 충족하는 경우

- 플래그가 지정된 각 레코드의 `SYSTEM-IP`, `private-ip` 및 `public-ip` 값을 신중하게 검토합니다

- 피어가 SD-WAN 제어 평면의 알려진 올바른 부분이 아닌지 확인합니다(클러스터 멤버, DR 사이트, 이전에 구성 요소에 할당된 IP 주소).
- 피어를 합법적인 것으로 식별할 수 없는 경우, 이는 잠재적인 보안 침해 지표를 나타낼 수 있습니다
- 모든 조사 결과를 문서화하고 즉시 TAC 케이스 열기
- 케이스에 전체 일치 피어 레코드 및 source 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 수집한 다음 모든 제어 구성 요소를 고정 소프트웨어 버전으로 업그레이드합니다. 업그레이드한 다음 TAC 케이스를 열고 관리 기술을 업로드하여 TAC에서 사용자의 환경에서 보안 침해 지표를 스캔할 수 있도록 합니다.

Q. 어떤 버전으로 업그레이드해야 합니까?

A. 최대한 빨리 가장 가까운 고정형으로 업그레이드해 주세요.

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: TAC 툴링을 사용하여 자동 스캔을 직접 수행할 수 있는 방법이 있습니까?

A : 고객은 Cisco 버그 ID CSCwt50498의 버그 검색 툴 페이지에 내장된 셀프 서비스 "버그 적용성 확인" 툴을 사용하여 제어 구성 요소에서 admin-techs를 다시 검사할 수도 있습니다.

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: 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 : 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: 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 TAC를 통해 지원을 받을 수 있습니다.

Q: 에지 라우터도 업그레이드해야 합니까?

A : 아니요. 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: 우리는 SD-WAN 클라우드(이전의 Cloud Delivered Cisco Catalyst SD-WAN[CDCS])에 있습니다. 어떤 버전으로 업그레이드할 예정입니까?

A : 현재 버전을 기준으로 SD-WAN 클라우드 클러스터는 현재 업그레이드 예정이거나 이미 고정 버전으로 업그레이드되었습니다. 다음은 SD-WAN Cloud(이전의 CDCS) 고정 릴리스입니다.

1. 조기 도입 클러스터 = 20.18.2.2(표준 릴리스와 동일)

2. 릴리스 클러스터 = 20.15.506(PSIRT 픽스가 있는 CDCS 특정 버전) 권장

SD-WAN 클라우드 고객은 이 PSIRT를 해결하기 위해 어떤 조치도 효과적으로 취할 필요가 없습니다.

Q: 공유 테넌트에 있습니다. 어떤 버전으로 업그레이드할 예정입니까?

A : 현재 버전을 기준으로 공유 테넌트는 현재 업그레이드 예정이거나 이미 고정 버전으로 업그레이드되었습니다. 다음은 공유 테넌트 고정 릴리스입니다.

1. 릴리스 클러스터 권장 = 20.15.5.2

Q: Cisco TAC는 이러한 취약점에 대한 포렌식 분석 또는 조사 서비스를 제공합니까?

A : Cisco TAC는 이러한 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 가이드를 참조하십시오.

Q: 시스템의 "루트" 사용자로부터 로그를 확인합니다. 이게 무슨 상관이야?

A : 그 당시 시스템에서 무슨 일이 일어나고 있는지 확인해 보세요. 이러한 로그는 완전히 예상할 수 있습니다. 예를 들어, admin-techs가 생성될 때 "루트" 사용자의 시스템 로그인 변경 로그가 표시됩니다. 재부팅 중에 "루트" 사용자에서도 로그를 볼 수 있습니다.

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

        user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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.