Monitoraggio e aggiornamento di Catalyst SD-WAN Security Advisory - Febbraio 2026

Sommario

Introduzione

Questo documento descrive i passaggi per identificare e correggere le vulnerabilità critiche della sicurezza in SD-WAN in base agli advisory PSIRT del 25 febbraio 2026.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Componenti di controllo e architettura SD-WAN Cisco Catalyst (vManage, vSmart, vBond)
- Procedura di aggiornamento di Cisco Catalyst SD-WAN
- Procedure di gestione dei casi TAC e raccolta di dati admin-tech Cisco

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per informazioni dettagliate e gli ultimi aggiornamenti, consultare la pagina ufficiale di consulenza PSIRT.

Queste avvertenze sono disponibili ai seguenti link:

- Vulnerabilità di Cisco Catalyst SD-WAN
- Vulnerabilità del bypass dell'autenticazione del controller SD-WAN Cisco Catalyst

I seguenti problemi sono risolti dai consigli PSIRT:

- ID bug Cisco CSCws5272
- ID bug Cisco CSCws3583
- ID bug Cisco CSCws3584
- ID bug Cisco CSCws3585
- ID bug Cisco CSCws3586
- ID bug Cisco CSCws3587
- ID bug Cisco CSCws93470

Panoramica sul flusso di lavoro di risoluzione

Nota: Tutte le implementazioni SD-WAN sono vulnerabili e richiedono un'azione immediata. Tuttavia, non tutti i sistemi mostrano segni di compromessi.

Azione richiesta: Apri una richiesta Cisco TAC per risolvere questo avviso di sicurezza.

Il TAC è disponibile per:

- Valutare l'ambiente per individuare eventuali indicatori di compromissione
- Guida l'utente attraverso il percorso di correzione appropriato in base alla valutazione
- Collaborare con il team PSIRT se vengono individuati indicatori di compromissione
- Fornire assistenza e supporto per l'aggiornamento se non vengono rilevati indicatori di compromissione

1. Collect Admin-Techs - Eseguire admin-tech su tutti i componenti di controllo (vSmart, vManage, vBond). Gli admin-tech vSmart non devono essere eseguiti simultaneamente, ovvero eseguiti uno alla volta. Tutti gli altri possono essere raccolti in qualsiasi ordine. Selezionare le opzioni Log and Tech. Core non è richiesto.
2. Apri una richiesta TAC - Contatta Cisco TAC e fornisci tutti i pacchetti di log Admin-tech per i componenti di controllo
3. Valutazione TAC - TAC valuta l'ambiente del cliente per rilevare eventuali indicatori di compromesso
4. Execute Remediation - Completa il processo specifico fornito da TAC

Passaggio 1: Raccolta dei file Admin-Tech da tutti i componenti di controllo

Obbligatorio: Raccogliere i file admin-tech da tutti i componenti di controllo prima di aprire la richiesta TAC. Questa operazione è essenziale per consentire a TAC di valutare l'ambiente.

Raccolta:

Nota: Per la generazione admin-tech, selezionare Log and Tech options (Opzioni registro e tecnologia). Core non è richiesto.

---

1. Esecuzione di admin-tech su TUTTI i controller (vSmarts) - non eseguirli simultaneamente; raccogli uno alla volta
2. Esegui admin-tech su TUTTI i manager (vManage)
3. Esegui admin-tech su TUTTE le convalide (vBonds)

Nota: Gli admin-tech vSmart non devono essere eseguiti contemporaneamente: è necessario raccoglierli uno alla volta. Gli admin-tech per manager e validatori possono essere raccolti in qualsiasi ordine.

Raccolta di informazioni su Admin-Tech in un ambiente SD-WAN e caricamento nella richiesta TAC

Nota: TAC analizza questi file per valutare l'ambiente in uso e individuare eventuali compromessi e individuare il percorso di correzione appropriato.

Alternativa: Verifica manuale (solo se non è possibile raccogliere dati relativi

all'amministrazione tecnica)

Per coloro che non possono condividere i file admin-tech, sono disponibili procedure di verifica manuali. Queste fasi forniscono indicatori preliminari che devono essere documentati e condivisi con il TAC.

Per le procedure dettagliate, vedere la sezione "Fasi della verifica manuale" alla fine di questo documento. Documentare tutti i risultati e fornirli a TAC nella richiesta di assistenza.

Passaggio 2: Apri una richiesta TAC e carica i file Admin-Tech

Dopo aver raccolto tutti i file admin-tech dal passaggio 1, aprire una richiesta di assistenza in Cisco TAC.

Azioni richieste:

1. Apri una richiesta TAC con un livello di gravità appropriato all'impatto aziendale
2. Caricare TUTTI i bundle di log admin-tech raccolti nel Passo 1 (Controller, Manager e Convalide)
3. Fare riferimento agli avvisi PSIRT
4. Attendere la valutazione e le indicazioni relative al TAC

Attenzione: TAC determina lo stato del sistema e consiglia le fasi successive da eseguire.

Non tentare ulteriori passaggi senza linee guida TAC

Passaggio 3: Valutazione TAC

TAC analizza i file admin-tech caricati e determina lo stato del sistema.

Durante questo periodo:

- Attendere una valutazione ufficiale del TAC prima di intraprendere qualsiasi azione
- TAC contatta l'utente con i risultati e le fasi successive

Passaggio 4: Esegui monitoraggio e aggiornamento (guidato da TAC)

TAC assiste l'utente nel processo di correzione appropriato in base alla valutazione effettuata. Completare tutte le istruzioni fornite da TAC.

Percorso A: Nessun indicatore di compromesso trovato - Aggiornamento

Se TAC conferma l'assenza di compromessi, eseguire l'aggiornamento alla versione software fissa. Selezionare la versione appropriata dalla tabella Versioni software fisso di questo documento e fare riferimento alla guida all'aggiornamento collegata in questa sezione.

Avviso: L'aggiornamento deve rimanere all'interno della versione principale corrente. Non eseguire l'aggiornamento a una versione principale più elevata senza una guida TAC esplicita.

Aggiornamento dei controller SD-WAN con l'utilizzo di vManage GUI o CLI

Percorso B: Indicatori di compromesso individuati - Guida PSIRT

Se TAC conferma la presenza di indicatori di compromissione, si rivolge al team PSIRT per sviluppare una strategia di correzione personalizzata specifica per l'ambiente in uso. Completare tutte le indicazioni fornite da TAC e PSIRT.

Versioni software fisse

Queste versioni software contengono correzioni per le vulnerabilità identificate:

Si applica alle versioni correnti	Versione corretta	Software disponibile
20,3, 20,6, 20,9	20.9.8.2 *	Link disponibile 2/27
20.10, 20.11, 20.12.5 e precedenti nella 20.12	20.12.5.3	20.12.5.3 aggiornamento delle immagini per vManage, vSmart e vBond
20.12.6	20.12.6.1	20.12.6.1 aggiornamento delle immagini per vManage, vSmart e vBond
20.13, 20.14, 20.15	20.15.4.2	20.15.4.2 aggiornamento delle immagini per vManage, vSmart e vBond
20.16, 20.17, 20.18	20.18.2.1	20.18.2.1 aggiornamento delle immagini per vManage, vSmart e vBond

---

Nota: Per i clienti su CDCS (Cisco-Hosted Cluster), la versione 20.15.405 è anche una

---

versione fissa. Ciò è valido in modo specifico per l'installazione di cluster ospitati da Cisco e viene gestito separatamente dal percorso di aggiornamento standard indicato sopra.

---

* Se la release è 20.9 o precedente: Il software fisso per la versione in uso (20.9.8.2) è disponibile a partire dal 2/27. Cisco consiglia di rimanere nella versione principale corrente e di attendere la versione 20.9.8.2 invece di effettuare l'aggiornamento a una versione principale più recente (20.12, 20.15, 20.18). Se la versione corrente è precedente alla 20.9, attendere la versione 20.9.8.2 per eseguire l'aggiornamento. Continuare a lavorare con TAC e verificare nuovamente il 27/20 per il collegamento software disponibile.

Riferimenti importanti:

- Matrice di aggiornamento
- Matrice di compatibilità dei controller

Appendice: Fasi di verifica manuale (solo se la raccolta di dati Admin-Tech non è possibile)

Nota: L'insieme Admin-tech è il metodo preferito e consigliato. Utilizzare la verifica manuale solo se non è assolutamente possibile raccogliere e condividere file admin-tech. Se non è possibile raccogliere i file admin-tech, eseguire la procedura manuale descritta di seguito per raccogliere gli indicatori preliminari per il calcolo del TAC.

Nota:

- Questi passaggi forniscono solo dati preliminari
- La raccolta di dati tecnici da parte dell'amministratore è fortemente preferibile per una valutazione accurata
- Documentazione delle scoperte e condivisione delle stesse con TAC nella richiesta di assistenza
- Il TAC determina la valutazione ufficiale

Requisiti: Queste operazioni devono essere eseguite su tutti i componenti di controllo.

Verifica 1: Verifica della presenza di account di accesso SSH non autorizzati nei log di autenticazione

Passaggio 1: Identificazione di IP di sistema vManage validi

Accedere a ciascun controller vSmart ed eseguire:

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

Output di esempio:

```
                                                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
```

Passaggio 2: Genera stringa espressione regolare (solo vBond e vSmart)

Combinare tutti gli IP di sistema della Fase 1 in un modello regex OR:

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

Fase 2b: Passaggio aggiuntivo per i sistemi vManage

Se si eseguono questi comandi su vManage stesso, aggiungere al regex l'indirizzo IP dell'host locale (127.0.0.1), l'indirizzo IP del sistema locale, tutti gli indirizzi IP del cluster e l'indirizzo IP dell'interfaccia di trasporto VPN 0:

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

Per trovare l'indirizzo IP del sistema vManage locale, utilizzare:

```
show control local-properties
```

Per trovare l'IP dell'interfaccia di trasporto VPN 0 e l'IP del cluster, utilizzare:

```
show interface | tab
```

Passaggio 3: Esegui comando di verifica

Eseguire questo comando, sostituendo REGEX con la stringa regex del passaggio 2:

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

Nota: Questo comando filtra i log di autenticazione per visualizzare solo gli account di accesso manage-admin da origini impreviste. Gli accessi legittimi devono provenire solo da IP correlati a vManage.

Passaggio 4: Interpreta risultati e documento per TAC

Se non viene visualizzato alcun output:

- Nessun indicatore di compromissione rilevato nel dispositivo
- Documentare questo risultato per la richiesta TAC
- Continuare la valutazione dei controller rimanenti

Se vengono stampate le righe del log:

- Esaminare attentamente tutti gli indirizzi IP visualizzati
- Verificare che l'indirizzo IP non sia correlato all'infrastruttura vManage (IP cluster, IP sistema precedente o simile)
- Se non si riesce a identificare l'IP di origine come legittimo, ciò può indicare potenziali indicatori di compromissione
- La voce registrata nel log mostra un timestamp e un indirizzo IP di origine
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere le voci di log, i timestamp e gli IP di origine nel caso
- Il TAC determina la valutazione ufficiale

Verifica 2: Verifica la presenza di connessioni peer non autorizzate nei syslog dei controller

Questo comando estrae tutte le coppie peer-type e peer-system-ip dai file syslog del controller e li invia come elenco da rivedere. Non contrassegna automaticamente le voci sospette: è necessario ispezionare l'output e determinare se ogni IP del sistema peer è una parte nota e legittima dell'infrastruttura SD-WAN. Eseguire questa operazione su tutti i componenti di controllo (Controller, Manager e Convalide).

Passaggio 1: Eseguire il comando su ciascun componente di controllo:

Accedere innanzitutto a vshell e quindi alla directory di log:

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

Eseguire quindi il comando seguente:

```
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
```

Passaggio 2: Interpreta risultati e documento per TAC

Se l'output mostra solo gli IP di sistema vManage/vSmart/vBond noti:

- Nessun indicatore di compromissione rilevato da questo controllo
- Documentare questo risultato per la richiesta TAC
- Continuare la valutazione dei componenti di controllo rimanenti

Se l'output contiene indirizzi IP di sistemi peer non riconosciuti:

- Esaminare attentamente tutti gli indirizzi IP e i tipi di peer visualizzati
- Verificare che l'indirizzo IP non sia correlato all'infrastruttura del control plane SD-WAN
- Se non si riesce a identificare l'IP di origine come legittimo, ciò può indicare potenziali indicatori di compromissione
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere l'output completo del comando con le coppie peer-type e peer-system-ip nel proprio caso
- Il TAC determina la valutazione ufficiale

Domande frequenti

Q: Qual è il primo passo per affrontare questo advisory della sicurezza? A: Raccogliere i file admin-tech da tutti i componenti di controllo e aprire una richiesta TAC per caricare i file. TAC valuta l'ambiente e fornisce indicazioni sulle fasi successive.

Q: È necessario raccogliere gli admin-tech da tutti i componenti di controllo? A: Sì, TAC richiede file admin-tech da tutti i controller (vSmart, raccolti uno alla volta), da tutti i manager (vManage) e da tutti i validatori (vBond) per valutare correttamente l'ambiente.

Q: In che modo TAC determina se il sistema è stato compromesso? A: TAC analizza i file admin-tech utilizzando strumenti specializzati per valutare l'ambiente del cliente alla ricerca di indicatori di compromesso.

Q: Cosa succede se vengono individuati indicatori di compromesso? A: TAC coinvolge il team PSIRT e contatta l'utente per discutere le fasi successive e le linee guida specifiche per l'ambiente in uso. Cisco non esegue il monitoraggio e l'aggiornamento per conto dell'utente. TAC offre le linee guida necessarie per procedere.

Q: Come è possibile sapere quale versione software fissa utilizzare? A: Fare riferimento alla tabella Versioni software fisso in questo documento. TAC conferma la versione appropriata per l'ambiente specifico.

Q: È possibile avviare l'aggiornamento prima che TAC analizzi gli esperti tecnici? A: No, attendere il completamento della valutazione di TAC e fornire indicazioni prima di intraprendere qualsiasi azione correttiva.

Q: Durante il monitoraggio e l'aggiornamento è previsto il downtime? A: L'impatto dipende dall'architettura di distribuzione e dal percorso di correzione. TAC fornisce indicazioni per ridurre al minimo l'impatto dei servizi durante il processo.
Q: Le correzioni PSIRT sono incluse nella release 20.15.5 e in altre release future? R: Sì, le correzioni sono incluse nella versione 20.15.5 e in altre versioni future. Tuttavia, è necessario assegnare IMMEDIATAMENTE una priorità all'aggiornamento per ridurre le vulnerabilità descritte in questo documento. (Non attendere!)

Q: È necessario aggiornare tutti i controller se non vengono rilevati indicatori di compromissione? A: Sì, tutti i componenti di controllo SD-WAN (vManage, vSmart e vBond) devono essere aggiornati a una versione software fissa. Non è sufficiente aggiornare solo un sottoinsieme di controller.

Q: Ho un overlay SD-WAN ospitato dal cloud. Quali sono le opzioni per l'aggiornamento? A: Per le sovrapposizioni ospitate nel cloud, i clienti hanno due opzioni:

1. Verificare se l'ambiente è pianificato per un aggiornamento automatico passando a SSP > Dettagli sovrapposizione > Finestre di modifica.
2. Se non si desidera attendere l'aggiornamento pianificato, sono disponibili due opzioni:
    - Eseguire l'aggiornamento autonomamente utilizzando le guide all'aggiornamento disponibili in questo documento.
    - Apri una richiesta TAC con la finestra di manutenzione preferita e TAC guida l'utente nel processo di aggiornamento.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).