

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica sul flusso di lavoro di risoluzione](#)

[Passaggio 1: Raccogli i file Admin-Tech da tutti i responsabili](#)

[Alternativa: Verifica manuale \(solo se non è possibile raccogliere dati relativi all'amministrazione tecnica\)](#)

[Passaggio 2: Aggiorna a una versione software fissa](#)

[Passaggio 3: Apri una richiesta TAC e carica i file Admin-Tech per la scansione](#)

[Passaggio 4: Se viene individuato un compromesso — Guida TAC](#)

[Versioni software fisse](#)

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

[Come identificare gli indicatori di compromesso](#)

[Verifica 1: Controlla il log degli accessi proxy del servizio](#)

[Verifica 2: Controllare il registro di Manager Server](#)

[Domande frequenti](#)

Introduzione

Questo documento descrive le fasi per identificare e correggere una vulnerabilità di sicurezza SD-WAN critica secondo le date di consulenza PSIRT del 30 settembre 2026. Cisco consiglia vivamente di eseguire l'aggiornamento a una versione software fissa per risolvere questo problema.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Componenti di controllo e architettura SD-WAN Cisco Catalyst (Manager, Controller e Validator)
- 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.

Questo avviso è disponibile al seguente collegamento:

- [Vulnerabilità del bypass dell'autenticazione dell'API di Cisco Catalyst SD-WAN Manager](#) (CVE-2026-76504, CWE-177). Valutazione impatto sulla sicurezza: Critico (punteggio base CVSS 9.8).

Questo difetto viene affrontato dal seguente advisory PSIRT:

- ID bug Cisco [CSCww79570](#)

Questo avviso ha effetto su Cisco Catalyst SD-WAN Manager (vManage).

Panoramica sul flusso di lavoro di risoluzione



Nota: Tutti i manager SD-WAN (vManage) che eseguono una release precedente alla prima versione fissa sono vulnerabili e richiedono un aggiornamento immediato. Tuttavia, non tutti i Catalyst Manager mostrano segni di compromesso.

Azione richiesta: È possibile raccogliere gli admin-tech da tutti i Catalyst SD-WAN Manager, aggiornare il sistema a una versione fissa e aprire una richiesta TAC per Cisco, in modo che TAC possa analizzare gli admin-tech e trovare eventuali compromessi.

Il TAC è disponibile per:

- Analizza gli admin-tech forniti per trovare gli indicatori di compromissione
- Fornire supporto per l'aggiornamento in caso di problemi durante l'aggiornamento
- Fornire indicazioni su ulteriori soluzioni se vengono identificati indicatori di compromissione

1. Collect Admin-Techs - Eseguire admin-tech su tutti i Catalyst SD-WAN Manager, inclusi tutti

i nodi di un cluster e di un'installazione di disaster recovery (DR), prima dell'aggiornamento per evitare la perdita dei dati di diagnostica. Selezionare le opzioni Log and Tech. Core non è richiesto.

2. Aggiorna a versione fissa - Aggiorna tutti i manager (vManage) a una versione software fissa elencata nella tabella [Versioni software fisso](#).



Nota: Non attendere i risultati dell'analisi TAC prima di eseguire l'aggiornamento. L'aggiornamento a una release fissa è la priorità più alta e chiude la vulnerabilità. La scansione TAC alla fase 3 determina se sono necessarie ulteriori azioni dopo l'aggiornamento.

3. Apri una richiesta TAC e carica Admin-Techs per cercare gli indicatori di compromissione - Apri una richiesta TAC di Cisco e carica tutti i bundle di log admin-tech raccolti nel passaggio 1. TAC analizza gli admin-tech per trovare gli indicatori di compromissione.
4. Se viene individuato un compromesso, utilizzare la guida TAC - Se TAC identifica indicatori di compromesso nell'ambiente, completare tutte le linee guida per la risoluzione dei problemi fornite da TAC. Se non vengono rilevati indicatori di compromissione, non è necessaria un'ulteriore azione oltre all'aggiornamento.

Passaggio 1: Raccogli i file Admin-Tech da tutti i responsabili

Obbligatorio: Raccogliere i file admin-tech da tutti i manager (vManage) prima di eseguire l'aggiornamento per evitare la perdita dei dati di diagnostica. Questi file vengono utilizzati da TAC nel passaggio 3 per analizzare l'ambiente alla ricerca di indicatori di compromissione.

Raccolta:



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

1. Eseguire admin-tech su ALL Manager (vManage).
2. Se i manager vengono eseguiti come cluster, eseguire admin-tech su ogni membro del cluster.
3. Se si dispone di un'implementazione di disaster recovery (DR), eseguire admin-tech su ogni Manager sia nel sito principale che in quello di disaster recovery.

[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: Aggiorna a una versione software fissa

Dopo aver raccolto gli admin-tech nella fase 1, aggiornare tutti i manager (vManage) a una versione software fissa.



Importante: Non attendere i risultati dell'analisi TAC prima di eseguire l'aggiornamento. L'aggiornamento a una release fissa è la priorità più alta e chiude la vulnerabilità. La scansione TAC alla fase 3 determina se sono necessarie ulteriori azioni dopo l'aggiornamento.

Selezionare la versione appropriata dalla tabella [Versioni software fisso](#) in questo documento.



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](#)



Nota: In caso di problemi durante l'aggiornamento, aprire una richiesta TAC per ottenere supporto per l'aggiornamento.

Passaggio 3: Apri una richiesta TAC e carica i file Admin-Tech per la scansione

Dopo l'aggiornamento alla Fase 2, aprire una richiesta di assistenza in TAC e caricare i file admin-tech raccolti nella Fase 1. TAC analizza gli admin-tech per rilevare eventuali indicatori di compromesso.

Azioni richieste:

1. Aprire una richiesta TAC di gravità 3 con l'ID CVE "CVE-2026-76504" nel titolo per avviare il processo di scansione.
2. Caricare TUTTI i bundle di log admin-tech raccolti nel passo 1 (tutti i manager, inclusi cluster e nodi DR).
3. Attendere che TAC completi l'analisi e comunichi i risultati.



Nota: TAC analizza i file admin-tech e comunica i risultati della scansione. Se non vengono rilevati indicatori di compromissione, non è necessaria un'ulteriore azione oltre all'aggiornamento.

Passaggio 4: Se viene individuato un compromesso — Guida TAC

Se TAC identifica degli indicatori di compromissione nell'ambiente, TAC contatta l'utente con istruzioni specifiche per la risoluzione dei problemi. Completare tutte le istruzioni fornite da TAC.

Se non vengono individuati indicatori di compromissione, l'aggiornamento completato nella fase 2 è sufficiente e non sono necessarie ulteriori correzioni.

Versioni software fisse

Queste versioni software contengono la correzione per questa vulnerabilità. Passate alla prima release fissa del treno di rilascio corrente.

Software Cisco Catalyst SD-WAN	Prima release fissa	Software disponibile
Precedente a 20.9 ¹	Eseguire la migrazione a una release fissa.	
20.9	20.9.10.1	20.9.10.1 immagini di aggiornamento per vManage
20.12	20.12.8.2	20.12.8.2 immagini di aggiornamento per vManage

Software Cisco Catalyst SD-WAN	Prima release fissa	Software disponibile
20.15	20.15.6.1	20.15.6.1 immagini di aggiornamento per vManage
20.18	20.18.4.1	20.18.4.1 immagini di aggiornamento per vManage
26.1	26.1.2.1	26.1.2.1 aggiornamento delle immagini per vManage
26.2	26.2.1	26.2.1 immagini di aggiornamento per vManage

¹ Fino alla fine della manutenzione del software. Cisco incoraggia vivamente i clienti ad effettuare l'aggiornamento a una versione supportata.

Il Cisco Product Security Incident Response Team (PSIRT) convalida solo le informazioni sulla versione interessate e quella fissa documentate nell'avviso.



Nota: Cisco ha risolto questa vulnerabilità anche in Cisco SD-WAN Cloud (Cisco Managed) versione 20.15.605, basato su cloud. Non è richiesta alcuna azione da parte dell'utente. I clienti possono determinare lo stato di monitoraggio e aggiornamento o la versione del software utilizzando la funzione Help nell'interfaccia utente del servizio.

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 responsabili (vManage), inclusi tutti i membri del cluster e tutti i responsabili di un sito di disaster recovery (DR). Accedere ai file di log da vshell (vshe11 dalla CLI di Manager) ed esaminare i file di log correnti e ruotati.

Come identificare gli indicatori di compromesso

Questo comitato consultivo ha due indicatori di compromesso. Entrambi fanno riferimento a voci per j_security_check in cui un carattere della richiesta è codificato (ad esempio /%6a_security_check) da indirizzi IP sconosciuti o non autorizzati.



Importante: Gli esempi in questa sezione mostrano l'utilizzo di %6a come carattere codificato j nella richiesta. Questo è solo un esempio e la vulnerabilità consente di utilizzare qualsiasi carattere codificato nella richiesta.



Nota: I sistemi Cisco Catalyst SD-WAN Manager esposti a Internet e le cui porte sono esposte a Internet rischiano di essere compromessi. In alcuni casi, questi indicatori di compromissione possono verificarsi durante le operazioni standard. Pertanto, devono essere valutati rispetto alla normale postura di rete per identificare ed evitare falsi positivi.

Indicatore	File di log	Che cosa significa	Verifica
Ricevuta richiesta j_security_check codificata	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	Un client ha inviato una richiesta di questo tipo al Manager.	Verifica 1
Codificata j_security_check richiesta elaborata per un utente viptela-	/var/log/nms/vmanage-server.log*	Il responsabile ha elaborato una richiesta di questo	Verifica 2

Indicatore	File di log	Che cosa significa	Verifica
Reserved-* utente		tipo per un utente riservato a viptela-* (un account del servizio di sistema riservato).	

Verifica 1: Controlla il log degli accessi proxy del servizio

Controllare il file `serviceproxy-access.log`, disponibile in `/var/log/nms/containers/service_proxy/serviceproxy-access.log`, per le voci relative a `j_security_check` provenienti da indirizzi IP sconosciuti o non autorizzati, come mostrato nell'esempio seguente:

```
[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
```

Alcuni file di registro nel sistema vManage sono limitati rispetto all'accesso alla directory principale e non possono essere utilizzati direttamente dai clienti. Per esaminare questi registri, i clienti devono generare un file `admin-tech`.

Interpreta risultati e documento per TAC

Se non vengono trovate voci di questo tipo:

- Nessun indicatore di compromissione rilevato in questo registro su questo gestore
- Documentare questo risultato per la richiesta TAC
- Continuare con la verifica 2, quindi ripetere entrambe le verifiche sui manager rimanenti

Se vengono trovate voci di questo tipo:

- Esaminare attentamente tutti gli indirizzi IP di origine visualizzati
- Cercare voci da indirizzi IP sconosciuti o non autorizzati. Verificare se l'IP di origine appartiene a un'attività autorizzata nell'ambiente (ad esempio, un'analisi della vulnerabilità o un test di penetrazione che viene eseguito)
- 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 le voci di log, i timestamp, gli IP di origine e i codici di stato HTTP nel caso specifico
- Il TAC determina la valutazione ufficiale

Verifica 2: Controllare il registro di Manager Server

Controllare il file `manage-server.log`, disponibile in `/var/log/nms/vmanage-server.log`, per individuare le voci correlate a `j_security_check` provenienti da indirizzi IP sconosciuti o non autorizzati, in modo specifico chiamate per utenti che includono nomi che iniziano con `viptela-Reserved-`, come mostrato nell'esempio seguente:

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



Nota: Gli account dei servizi di sistema riservati per `viptela` sono documentati nella sezione Authentication, Authorization, and Accounting della Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide.

Interpreta risultati e documento per TAC

Se non vengono trovate voci di questo tipo:

- Nessun indicatore di compromissione rilevato in questo registro su questo gestore
- Documentare questo risultato per la richiesta TAC
- Ripeti entrambe le verifiche sugli altri manager

Se vengono trovate voci di questo tipo:

- Ciò può indicare potenziali indicatori di compromissione
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere le voci di registro e i timestamp nel caso, insieme ai risultati della verifica 1 per lo stesso periodo di tempo
- 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 manager (vManage), quindi aggiornare tutti i manager a una versione software fissa. Dopo l'aggiornamento, aprire una richiesta TAC e caricare gli `admin-tech` in modo che TAC possa analizzare l'ambiente per rilevare eventuali indicatori di compromesso.

Q: Quali componenti sono interessati da questo avviso?

A: Il problema riguarda solo Cisco Catalyst SD-WAN Manager (vManage).

Q: È necessario aggiornare anche i controller, i validator o i router perimetrali?

A: No, per non rispondere a questo avviso. Aggiornare tutti i manager (vManage) a una versione fissa e utilizzare la [matrice di compatibilità dei controller](#) per verificare che la nuova versione di manager sia compatibile con gli altri componenti.

Q: È disponibile una soluzione alternativa?

A: No. Non esistono soluzioni alternative per risolvere questa vulnerabilità. Eseguire l'aggiornamento a una versione fissa.

Q: A quale versione devo eseguire l'aggiornamento?

A: Passate al primo rilascio fisso nel vostro treno di rilascio corrente il prima possibile. Fare riferimento alla tabella [Versioni software fisso](#) in questo documento. TAC conferma la versione appropriata per l'ambiente specifico.

Q: Ho già effettuato l'aggiornamento a una versione fissa per una precedente consulenza sulla sicurezza SD-WAN. È necessario eseguire di nuovo l'aggiornamento?

A: Sì, a meno che la release corrente non sia uguale o successiva alla prima release fissa nella tabella [Versioni software fisso](#). Le versioni corrette per gli advisory precedenti non includono necessariamente la correzione per questa vulnerabilità.

Q: Devo raccogliere gli admin-tech da tutti i responsabili?

A: Sì. TAC richiede file admin-tech da ogni Manager (vManage), inclusi tutti i membri del cluster e tutti i Manager in un sito di disaster recovery (DR), per valutare correttamente l'ambiente.

Q: Posso cercare da solo degli indicatori di compromesso?

A: Sì. Se non è possibile raccogliere i file admin-tech, eseguire la [procedura di verifica manuale](#) su ciascun Manager e condividere i risultati con TAC. La raccolta di dati tecnici per gli amministratori rimane il metodo preferito, mentre il TAC determina la valutazione ufficiale.

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 ti contatta per discutere le fasi successive e le linee guida specifiche per il tuo ambiente. Cisco non esegue il monitoraggio e l'aggiornamento per conto dell'utente. TAC offre le linee guida necessarie per procedere.

Q: È possibile avviare l'aggiornamento prima che TAC analizzi gli esperti tecnici?

A: Sì. Raccogliere dati tecnici da un amministratore, eseguire l'aggiornamento a una versione fissa e aprire una richiesta TAC per analizzare i dati tecnici da un amministratore e individuare eventuali

indicatori di compromissione.

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: 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.
 - Aprire una richiesta TAC di standby per la finestra di manutenzione preferita. TAC è disponibile per l'assistenza in caso di problemi con l'aggiornamento.

Q: Siamo una sovrapposizione ospitata da Cisco. È necessario rivedere le regole di accesso alla SSP?

A: Tutti i clienti ospitati da Cisco sono invitati a rivedere le proprie regole connessioni in SSP > Sovrapposizioni dettagli > Consenti regole connessioni in entrata e ad accertarsi che siano consentiti solo i prefissi necessari dal lato dell'utente. Queste regole sono valide solo per l'accesso alla gestione e non si applicano ai router edge.

Q: Cisco TAC fornisce servizi di analisi o investigazione forense per risolvere questa vulnerabilità?

A: Cisco TAC può assistere i clienti nella ricerca di Indicatori di compromessi (IoC) relativi a questa vulnerabilità. TAC non esegue tuttavia analisi forensi approfondite né indagini sugli incidenti. Per un lavoro di consulenza legale completo o per indagini dettagliate sulla sicurezza, si consiglia ai clienti di rivolgersi alla società di terze parti per la gestione degli incidenti.

Q: Quali sono le best practice generali o i modi per ridurre le vulnerabilità per la mia sovrapposizione SD-WAN?

A: Per le best practice e i consigli per ridurre le vulnerabilità nella sovrapposizione SD-WAN, consultare la [Cisco Catalyst SD-WAN Hardening Guide](#).

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).