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

Sommario

Introduzione

Questo documento descrive i passaggi per identificare e affrontare le vulnerabilità critiche della sicurezza in SD-WAN in base agli advisory PSIRT del 4 giugno 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 dell'escalation dei privilegi autenticati del gestore Cisco Catalyst SD-WAN

I seguenti problemi sono risolti dai consigli PSIRT:

- ID bug Cisco CSCwu18563

Panoramica sul flusso di lavoro di risoluzione

Questo advisory descrive una vulnerabilità di escalation dei privilegi in SD-WAN Manager che richiede privilegi di netadmin da sfruttare.

Secondo l'advisory, i percorsi noti per ottenere tali privilegi da un utente remoto non autenticato sono lo sfruttamento di CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) o CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Se i componenti di controllo sono stati aggiornati a una versione fissa per entrambi gli admin-tech e Cisco non ha identificato alcun potenziale indicatore di compromissione (IoC) nei file admin-tech forniti per gli eventi precedenti, i percorsi di utilizzo non autenticati noti per questa nuova vulnerabilità vengono mitigati su tali dispositivi specifici, in base ai file esaminati.

Ciò non elimina l'esposizione quando un utente non autorizzato possiede credenziali netadmin valide. Cisco non ha ancora rilasciato una correzione software per questa vulnerabilità e non sono disponibili soluzioni alternative; seguiranno ulteriori orientamenti non appena saranno disponibili.

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

- Fornire orientamenti sulle prossime misure da adottare qualora siano individuati indicatori di compromesso

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: esecuzione di una valutazione preliminare degli indicatori di compromissione nell'ambiente del cliente e valutazione preliminare degli indicatori di compromissione nell'ambiente del cliente.
4. Esegui correzione: completare la procedura specifica fornita da TAC, se necessario.

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 qualsiasi aggiornamento o modifica della configurazione, in modo da preservare i dati diagnostici e gli eventuali indicatori di compromissione (IoC). Questi file vengono utilizzati da TAC nel passaggio 3 per analizzare l'ambiente.

Raccolta: per la generazione admin-tech, selezionare le opzioni Log and Tech. 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)

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 del cliente alla ricerca di indicatori di compromesso relativi a questo avviso. L'analisi di questo avviso si concentra su una voce specifica del registro che non fa distinzione tra uso legittimo e uso dannoso; è richiesta la revisione manuale tramite TAC.

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

Per i clienti che non possono condividere file admin-tech, è disponibile una procedura di verifica manuale. Questa procedura fornisce un indicatore preliminare che deve essere documentato e

condiviso con il TAC.

Per la procedura dettagliata, 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 i dati tecnici per l'amministratore nel passaggio 1, aprire una richiesta di assistenza in Cisco TAC e caricare i file tecnici per l'amministratore raccolti. TAC analizza gli admin-tech per individuare gli indicatori di compromesso associati a questo avviso.

Azioni richieste:

1. Aprire una richiesta TAC di gravità 3 con "CVE-2026-20245" e l'ID advisory `cisco-sa-sdwan-privesc-4uxFrdzx` nel titolo per avviare l'analisi.
2. Caricare TUTTI i bundle di log admin-tech raccolti nel Passo 1 (Controller, Manager e Convalide).
3. Attendere il completamento dell'analisi da parte di TAC e comunicare i risultati.

Nota: Cisco non ha rilasciato una correzione software per questa vulnerabilità e non sono disponibili soluzioni alternative. L'analisi TAC nel passaggio 3 aiuta a determinare se vi sono indicatori di compromissione nei file admin-tech forniti. Seguiranno ulteriori indicazioni man mano che saranno disponibili dal reparto di ingegneria.

Passaggio 3: Valutazione TAC

TAC esegue un'analisi preliminare dei file admin-tech caricati nella fase 2 e li valuta per rilevare eventuali indicatori di compromesso associati a questo avviso.

Per questo advisory, l'analisi è incentrata su una voce di log specifica in `/var/log/scripts.log` su ciascun Manager (vManage). Poiché il comando sottostante è legittimo e il registro non distingue tra utilizzo legittimo e dannoso, tutte le voci corrispondenti richiedono una revisione manuale da parte di TAC rispetto alla normale postura operativa del cliente prima di essere trattate come un indicatore confermato.

Possibili risultati dell'analisi TAC:

- Nessuna voce di log corrispondente identificata: in base ai file admin-tech esaminati, non sono stati osservati indicatori associati a questo advisory. Al momento non sono necessarie ulteriori azioni specifiche per questo parere. Il risultato è limitato ai file admin-tech ricevuti e può essere limitato dal periodo di conservazione del log su ciascun dispositivo.
- Voci del log corrispondenti identificate: TAC richiede al cliente ulteriori operazioni di revisione. Poiché Cisco non ha rilasciato una correzione software per questo advisory, il solo

aggiornamento non risolve questa vulnerabilità. Le linee guida di TAC per scenari di compromissione confermati sono documentate negli articoli correlati della TechZone di cui alla fase 4.

Nota: In base all'advisory, lo sfruttamento di questa vulnerabilità richiede privilegi netadmin, che un utente non autenticato può ottenere solo attraverso credenziali valide o lo sfruttamento di CVE-2026-20182 o CVE-2026-20127. Se i componenti di controllo sono stati aggiornati a una versione fissa per entrambi gli advisory e non sono stati identificati indicatori di compromissione per gli eventi precedenti, i percorsi di sfruttamento non autenticati noti per questa nuova vulnerabilità sono mitigati su tali dispositivi specifici, in base ai file esaminati.

Passaggio 4: Se vengono individuati indicatori di compromissione - seguire le istruzioni TAC

Se TAC identifica indicatori di compromissione associati a questo avviso nell'ambiente in uso, TAC contatta l'utente con indicazioni specifiche. Completare tutte le istruzioni fornite da TAC.

Se non vengono identificati indicatori di compromissione per questo avviso, non è al momento necessaria alcuna ulteriore azione specifica per questo avviso, sulla base dei file admin-tech esaminati.

Importante: Cisco non ha rilasciato una correzione software per questo avviso e non sono disponibili soluzioni alternative. Poiché lo sfruttamento di questa vulnerabilità richiede privilegi di netadmin ottenuti tramite CVE-2026-20182 o CVE-2026-20127, i clienti devono garantire la correzione di questi avvisi precedenti è completa. Fare riferimento ai documenti corrispondenti per il flusso di monitoraggio e aggiornamento stabilito:

Considerazioni

Al termine di un'azione correttiva riuscita e sulla base dei requisiti specifici di sicurezza di ciascun cliente, i clienti possono valutare e intraprendere le seguenti attività igieniche. Queste attività si applicano indipendentemente dall'opzione di correzione selezionata. Sono gestiti dal cliente; Cisco non li dirige né li esegue per conto del cliente.

- Verifica di tutti gli account utente locali
- Rotazione delle credenziali
- Rotazione di eventuali segreti presenti nelle configurazioni dei dispositivi, ad esempio (elenco non esaustivo):

    - Credenziali per gli account utente locali
    - Stringhe della community SNMP
    - Chiavi segrete TACACS
    - Chiavi e certificati VPN precondivisi
    - Chiavi SSH attendibili
- Revisione dei modelli di configurazione

Dispositivi perimetrali — Possibile compromissione

Cisco sconsiglia di specificare un percorso di ripristino; la scelta di un'opzione di risanamento spetta al cliente. Come nota informativa per i clienti che valutano il proprio ambiente: se il cliente sospetta la compromissione di un dispositivo periferico, un reset di fabbrica e il re-onboarding del dispositivo o dei dispositivi periferici interessati è un'azione gestita dal cliente che il cliente potrebbe voler prendere in considerazione quando effettua la selezione. La decisione di seguire questo approccio e la scelta dell'opzione da selezionare spetta al cliente.

Il comando corretto per eseguire un ripristino sicuro in fabbrica è:

```
factory-reset all secure 3-pass
```

Versioni software fisse

⚠ Importante: Al momento della pubblicazione di questo documento, Cisco non ha rilasciato una correzione software per CVE-2026-20245. In base all'advisory, Cisco prevede di risolvere questa vulnerabilità in Cisco Catalyst SD-WAN Manager in una versione futura. Non sono disponibili soluzioni alternative. Questa sezione verrà aggiornata quando sarà disponibile software fisso.

Poiché lo sfruttamento di questa vulnerabilità richiede privilegi di netadmin che un utente non autenticato può ottenere solo attraverso CVE-2026-20182 o CVE-2026-20127, i clienti sono incoraggiati a garantire che i loro componenti di controllo eseguano una versione fissa per tali avvisi precedenti. Le versioni fisse di questi avvisi sono documentate nel SD-WAN Security Advisory del 14 maggio 2026 e nel documento TechZone corrispondente:

- Vulnerabilità del bypass di autenticazione del controller SD-WAN Cisco Catalyst (14 maggio 2026)
- (tabella Versioni software fisse)

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: La raccolta Admin-tech è il metodo preferito. Utilizzare la procedura di verifica manuale descritta di seguito solo se non è possibile raccogliere e condividere i file admin-tech con TAC. Il risultato di questa operazione manuale è preliminare; documenta i risultati e li condivide con TAC, che effettua la valutazione ufficiale.

Nota: Per questo avviso, la verifica manuale consiste in un unico controllo mirato del registro. La voce del log cercata è generata da un comando legittimo e il solo log non distingue tra uso legittimo e dannoso. Prima di essere considerati un indicatore potenziale, i dati corrispondenti devono essere esaminati in base alla normale postura operativa del cliente. Se una voce corrispondente non può essere riconciliata con le normali operazioni, documentare il risultato e condividerlo con TAC.

Verifica: Verifica `scripts.log` su ogni manager (vManage) per voci di caricamento dell'elenco tenant

In base all'advisory PSIRT, i clienti sono incoraggiati a controllare il file `scripts.log`, che si trova in `/var/log/`, per le voci simili al seguente esempio:

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Passaggio 1: Accedere a vshell su ciascun Manager (vManage) ed eseguire una ricerca nel file di log

Dalla CLI di vManage, accedere alla shell ed eseguire:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Ripetere il controllo su ogni vManage della distribuzione (inclusi tutti i membri del cluster e gli eventuali vManage associati a DR).

Passaggio 2: Interpreta risultati e documento per TAC

Se NON vengono restituite voci corrispondenti:

- Nel file di log del dispositivo non sono stati rilevati indicatori di compromissione associati all'avviso.
- Documentare questo risultato per la richiesta TAC (includere il nome host del dispositivo e la data/intervallo dei file di registro cercati).
- Continuare il controllo sui manager rimanenti.

Se vengono restituite voci corrispondenti:

- Ogni voce corrispondente deve essere verificata rispetto alla normale postura operativa del cliente. Il comando sottostante (caricamento dell'elenco dei tenant) è legittimo e può essere visualizzato durante le operazioni di routine.
- Per ogni voce corrispondente, acquisire il timestamp, la riga di log completa e il percorso del file a cui si fa riferimento dopo il `percorso della riga successiva`.
- Se una voce corrispondente non può essere riconciliata con un'operazione nota e legittima, questo può essere un indicatore di compromissione. Documentare il risultato e inviarlo a TAC per la revisione.
- Documentazione di tutti i risultati e apertura di una richiesta TAC. Includere le voci di log corrispondenti e l'output del comando source nel caso specifico.
- TAC esegue la valutazione ufficiale. Se la valutazione identifica indicatori di compromissione, seguire il flusso descritto nei documenti correlati di TechZone: e guide ai rimedi.

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 (vSmart, vManage, vBond) prima di qualsiasi aggiornamento o modifica della configurazione per preservare i dati di diagnostica e qualsiasi potenziale indicatore di compromissione. Quindi, aprire una richiesta Cisco TAC e caricare gli admin-tech in modo che TAC possa analizzarli.

Q: Cisco ha rilasciato una correzione software per questa vulnerabilità?

A: Non al momento della pubblicazione del presente documento. In base all'advisory, Cisco prevede di risolvere questa vulnerabilità in Cisco Catalyst SD-WAN Manager in una versione futura. Non sono disponibili soluzioni alternative. Questo documento verrà aggiornato quando sarà disponibile una versione fissa.

Q: Se non è disponibile alcuna correzione, perché Cisco consiglia un'azione adesso?

A: Per sfruttare questa vulnerabilità sono necessari i privilegi netadmin. In base all'advisory, un utente non autenticato può ottenere tali privilegi solo attraverso credenziali valide o attraverso lo sfruttamento di CVE-2026-20182 o CVE-2026-20127. Garantendo che i componenti di controllo

siano aggiornati alle versioni fisse per tali advisory precedenti indirizzi i percorsi non autenticati noti per ottenere i privilegi necessari per sfruttare questa vulnerabilità. L'analisi admin-tech nella Fase 3 aiuta a determinare se vi sono indicatori di compromissione nei file esaminati.

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 eseguire l'analisi.

Q: In che modo TAC determina se il sistema dispone di indicatori di compromesso associati a questo avviso?

A: TAC esamina i file admin-tech e cerca la voce di registro specifica descritta nell'advisory di PSIRT all'indirizzo `/var/log/scripts.log` su ciascun Manager. Il comando sottostante è legittimo; qualsiasi voce corrispondente deve essere esaminata rispetto alla normale postura operativa prima di essere trattata come un indicatore potenziale. TAC esegue questa revisione.

Q: Cosa succede se vengono individuati indicatori di compromesso?

A: TAC contatta l'utente con indicazioni specifiche. Poiché non è attualmente disponibile alcuna correzione software per questo advisory, l'aggiornamento da solo non risolve un compromesso confermato. Le linee guida del TAC seguono il flusso documentato negli articoli relativi alla TechZone per i pareri del maggio 2026 e del febbraio 2026.

Q: Questo avviso riguarda i router perimetrali (Cisco IOS XE)?

A: Questo avviso ha effetto su Cisco Catalyst SD-WAN Manager. Secondo l'advisory, Cisco ha osservato alcuni casi limitati in cui lo sfruttamento di questa vulnerabilità ha portato a una modifica della configurazione trasferita ai dispositivi periferici; i clienti sono invitati a verificare la configurazione dei loro dispositivi edge.

Q: Quali tipi di distribuzione sono interessati?

A: In base all'advisory, questa vulnerabilità influisce su tutti i tipi di installazione di Cisco Catalyst SD-WAN Manager indipendentemente dalla configurazione del dispositivo, inclusa l'installazione locale, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed) e Cisco SD-WAN per enti pubblici (FedRAMP).

Q: Ho già effettuato l'aggiornamento per i consigli di maggio 2026 e febbraio 2026 e non sono stati identificati indicatori di compromesso per tali eventi. Sono esposto a questa nuova vulnerabilità?

A: Se i componenti di controllo eseguono una versione fissa sia per CVE-2026-20182 che per CVE-2026-20127 e non sono stati identificati indicatori di compromissione per gli eventi precedenti nei file admin-tech esaminati, i percorsi di sfruttamento noti non autenticati per questa nuova vulnerabilità vengono mitigati su tali dispositivi specifici, in base ai file esaminati. Ciò non elimina l'esposizione quando un utente malintenzionato possiede credenziali netadmin valide.

Q: È possibile eseguire personalmente la verifica anziché attendere il TAC?

A: I clienti che non possono condividere gli amministratori possono eseguire la procedura di verifica manuale descritta nell'Appendice. Il risultato è preliminare; documenta i risultati e li condivide con TAC, che effettua la valutazione ufficiale.

Q: Quali sono le best practice generali per rafforzare la mia sovrapposizione SD-WAN?

A: Per le best practice, consultare la guida alla protezione avanzata di Cisco Catalyst SD-WAN.

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

A: Cisco TAC può assistere i clienti revisionando i file admin-tech per gli indicatori di compromesso documentati nell'advisory PSIRT. Cisco TAC non esegue analisi forensi approfondite o indagini sugli incidenti. Per un lavoro legale completo o per indagini dettagliate sulla sicurezza, i clienti sono incoraggiati a rivolgersi alla loro società di terze parti preferita per la gestione degli incidenti.

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).