

Verifica la presenza di articoli esistenti in grassetto

Sommario

[Introduzione](#)

[Riferimenti — Documentazione di Cisco SD-WAN CVE-2026-20182](#)

[Messaggi di posta elettronica](#)

[Sherlock 1 - Aspirazione - Richiesta di aggiornamento e file Admin-Tech](#)

[Sherlock 2 - Risultato - Nessun IoC osservato \(per file\)](#)

[Sherlock 3 - Promemoria - File Admin-Tech mancanti](#)

[TAC 1 - Indagine - Necessaria ulteriore revisione \(sospetto IoC\)](#)

[TAC 2 - Risultato - Nessun IoC trovato \(confermato dal tecnico\)](#)

[TAC 3 - Convalida - Conferma proprietà IP in sovrapposizione](#)

[TAC 4 - Risultato - Falso positivo cancellato](#)

[TAC 5 - Critico - Identificato IoC, pianifica chiamata di revisione](#)

[TAC 6 - Risultato - IoC duplicato \(Close & Redirect\)](#)

[TAC 7 - Rimedio - Opzioni - Seguito \(dopo la chiamata\)](#)

[TAC 8 - Risanamento - Opzioni aggiornate per i fabric compromessi \(opzione 2 follow-up\)](#)

[TAC 17 - Risultato inverso - In precedenza non esisteva IoC, ora IoC identificato \(CVE-2026-20182\)](#)

[CloudOps 1 - Proattivo - Rilevato IoC nella scansione del cloud, richiesto Admin-Tech per la convalida](#)

[Messaggi di posta elettronica per la WAVE 2A per clienti precedentemente interessati che non hanno ancora completato le opzioni A, B o C. \(È necessario ripetere le opzioni 1 e 2\)](#)

[Modello TAC 9 senza IOC per PSIRT2a/sono stati ricostruiti \(precedentemente interessati\)](#)

[Modello TAC 10 per sì IOC per PSIRT2a/sono stati ricostruiti \(precedentemente interessati\)](#)

[Modello TAC 11 per nessun COI per PSIRT2a/non sono stati ricostruiti \(precedentemente interessati\)](#)

[Modello TAC 12 per sì IOC per PSIRT2a/non sono stati ricostruiti \(precedentemente interessati\)](#)

[E-mail per WAVE 2A per NUOVI clienti \(nessun impatto precedente\)](#)

[Modello TAC 13 per senza IOC/senza versione fissa disponibile \(WAVE 2a — Await Fix\)](#)

[Modello TAC 14 per rilascio fisso non disponibile \(WAVE 2a — Aggiorna ora\)](#)

[Modello TAC 15 per rilascio fisso identificato dal COI disponibile \(WAVE 2a — Urgent Upgrade\)](#)

[Modello TAC 16 per IOC identificato / non è disponibile alcuna versione fissa \(WAVE 2a — Harden & Await Fix\)](#)

Introduzione

Questo documento centralizza i modelli e-mail approvati dal cliente, utilizzati durante la selezione e la risoluzione dei problemi relativi alla vulnerabilità del bypass di autenticazione del controller

Cisco Catalyst SD-WAN. I modelli sono suddivisi per mittente: Sherlock (scambi automatizzati di casi che raccolgono dati admin-tech e restituiscono risultati preliminari dell'loC) e TAC Engineer (follow-up da parte dell'uomo per attività di indagine, convalida e correzione).

Riferimenti — Documentazione di Cisco SD-WAN CVE-2026-20182

Elenco principale di tutti i documenti Cisco a cui si fa riferimento nei modelli di e-mail precedenti. Numerazione unificata — apici per e-mail (es. [2]) selezionare le voci dell'elenco.

1. Guida per la protezione avanzata di Cisco SD-WAN — <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. Consulenza ufficiale sulla sicurezza (cisco-sa-sdwan-mltnps2-JxpWm7R) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. Guida alla risoluzione dei problemi relativi a TAC — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-hld--1516256622>
4. Guida all'aggiornamento di Cisco SD-WAN — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. Guida alla raccolta di dati Cisco SD-WAN Admin-Tech — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. Secondo consiglio per la sicurezza (cisco-sa-sdwan-rpa2-v69WY2SW) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. Avvio dell'aggiornamento di Catalyst SD-WAN — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

Messaggi di posta elettronica

Sherlock 1 - Aspirazione - Richiesta di aggiornamento e file Admin-Tech

Scenario d'uso

Sensibilizzazione iniziale quando un caso TAC è aperto per CVE-2026-20182 per consigliare la raccolta di dati admin-tech da e quindi l'aggiornamento di tutti i componenti di controllo SD-WAN.

Oggetto

Importante: Azione richiesta per CVE-2026-20182 - Pianificazione aggiornamento e valutazione loC

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC).

Per quanto riguarda la vulnerabilità associata a **CVE-2026-20182**, si prega di rivedere il [parere ufficiale sulla sicurezza](#)^[1] per informazioni dettagliate e la [guida per la risoluzione dei problemi di TAC](#)^[2].

Il nostro obiettivo principale è proteggere il vostro ambiente. La **pianificazione e l'esecuzione dell'aggiornamento rappresentano** la fase più critica per ridurre questo rischio. Se l'aggiornamento non è stato ancora pianificato, procedere immediatamente.

Risorse di aggiornamento: Per istruzioni dettagliate su come eseguire l'aggiornamento, consultare il seguente documento ufficiale di Cisco: [Guida all'aggiornamento di Cisco SD-WAN](#)^[3]

Per consentire la valutazione iniziale dell'ambiente per i potenziali indicatori di compromissione (IoC) relativi a CVE-2026-20182, è necessario eseguire una raccolta di admin-tech *prima* di eseguire l'aggiornamento. Attenersi a questo ordine di esecuzione:

- 1. Raccogli file Admin-Tech:** Generare i log admin-tech da tutti i componenti di controllo SD-WAN prima dell'aggiornamento per evitare la perdita dei dati di diagnostica. Accertarsi di selezionare sia **"Log"** che **"Tech"** durante la generazione di questi file.
 - **Smarts (controller):** Raccoglierne uno alla volta, non contemporaneamente.
 - **vBonds (validatori):** Raccogli da tutti i nodi.
 - **Manager (vManage):** Eseguire la raccolta da tutti i nodi nel cluster (DR attivo e in standby).
- 2. Esegui aggiornamento:** Aggiornare tutti i componenti di controllo SD-WAN (vManage, vSmart, vBond) a una versione software fissa elencata nell'advisory. Non attendere l'analisi del log admin-tech prima di iniziare l'aggiornamento, in quanto l'aggiornamento chiude immediatamente la vulnerabilità.
- 3. Carica in richiesta TAC:** Al termine dell'aggiornamento, se possibile, caricare contemporaneamente i file raccolti in precedenza nella richiesta TAC esistente. Il nostro team eseguirà quindi una scansione di questi log per valutare l'ambiente del cliente per gli Indicatori di Compromesso (IoC).

Risorse e supporto:

Per ulteriori dettagli e istruzioni dettagliate sulla generazione e l'invio sicuro dei file admin-tech, fare riferimento a questa guida: [Guida alla raccolta di dati Cisco SD-WAN Admin-Tech](#)^[4].

Se disponi di un abbonamento a BCS/LCS, contatta il tuo Cisco NCE o il tuo Delivery Manager per ricevere ulteriori informazioni sul processo di aggiornamento o sulle fasi successive.

La riservatezza e la sicurezza dei dati rimangono la nostra priorità principale. Tutte le informazioni fornite saranno gestite in conformità con le policy sulla privacy e sulla sicurezza di Cisco.

L'utente riceve una conferma automatica tramite e-mail per **CIASCUN** file caricato correttamente nella richiesta; controlla queste notifiche.

Grazie per aver collaborato tempestivamente alla sicurezza dell'infrastruttura.

Collegamenti:

[1] [Consulenza ufficiale sulla sicurezza](#)

[2] [Guida alla correzione del TAC](#)

[3] [Guida all'aggiornamento di Cisco SD-WAN](#)

[4] [Guida alla raccolta di Cisco SD-WAN Admin-Tech](#)

Distinti saluti,

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Sherlock 2 - Risultato - Nessun IoC osservato (per file)

Scenario d'uso

Inviato dopo che l'analisi admin-tech mostra nessun indicatore di compromissione osservato per un file caricato specifico. Inviato una volta per file elaborato.

Oggetto

Update: Risultati dell'analisi per il componente SD-WAN [Insert File Name] - CVE-2026-20182

Messaggio

Gentile Cliente,

Grazie per la vostra pazienza.

L'analisi del file admin-tech [Insert File Name] è stata completata. All'interno di tale file non sono stati identificati indicatori di compromissione relativi a CVE-2026-20182 per questo specifico dispositivo.

La quantità di dati di log recuperati e forniti a Cisco per questa revisione potrebbe essere stata limitata dal periodo di conservazione del log configurato in base alla **Cisco SD-WAN Hardening Guide**^[1].

Importante: Fasi successive e chiusura della richiesta:

1. **Attendi tutti i risultati:** I risultati in questa e-mail potrebbero essere parziali. Ogni file verrà analizzato come fornito. Attendere di aver ricevuto conferma per tutti i file caricati prima di considerare completata la valutazione.
2. **Priorità di aggiornamento:** Mentre le scansioni preliminari dei log admin-tech non hanno identificato gli indicatori di compromesso (IoC), la vulnerabilità sottostante può rimanere. Per le implementazioni Cisco Cloud-Pro e Cisco On-Prem, se non l'avete già fatto, assegnate la priorità all'aggiornamento completo dei componenti di controllo SD-WAN appena possibile.
 - Cisco Cloud (fka: SaaS) i fabric del cliente vengono aggiornati automaticamente da Cisco come parte del servizio gestito. Non è necessaria alcuna azione.
3. **Chiusura della richiesta:** Dopo aver ricevuto i risultati "no detected IoC" per tutti i file caricati E (se applicabile) dopo aver completato con successo l'aggiornamento del software nell'ambiente, è possibile considerare risolta la richiesta e procedere con le procedure standard di chiusura.

Aggiorna risorse (se applicabile): Per istruzioni dettagliate su come eseguire l'aggiornamento per Cisco Cloud-Pro e Cisco On-Prem, consultare il seguente documento ufficiale di Cisco: Guida all'aggiornamento di Cisco SD-WAN

Una panoramica di alto livello del processo di upgrade include:

1. Caricamento delle immagini software appropriate nel repository di Manager (vManage).
2. Aggiornamento sequenziale dei controller, a partire da Manager (vManage), seguito da Validator (vBond) e Controller (vSmart).
3. Attivazione delle nuove versioni del software e convalida delle funzionalità del sistema.

Continueremo a monitorare il tuo caso. Se non riceviamo risposta entro 10 giorni lavorativi dalla comunicazione di tutti i risultati sulla base dei file che abbiamo ricevuto da parte vostra, non riteniamo necessaria ulteriore assistenza e procediamo con le normali procedure di chiusura dei casi TAC. Se hai bisogno di aiuto in qualsiasi momento, faccelo sapere.

Distinti saluti,

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

⬇ Scarica modello .eml

Sherlock 3 - Promemoria - File Admin-Tech mancanti

Scenario d'uso

Follow-up automatico quando i file admin-tech inviati non corrispondono al numero di componenti di controllo SD-WAN trovati nei log.

Oggetto

Promemoria: File Admin-Tech mancanti necessari per la valutazione CVE-2026-20182

Messaggio

Gentile Cliente,

Mancano ancora gli admin-tech dai componenti di controllo SD-WAN, quindi il nostro sistema non è in grado di valutare alcun Indicatore di Compromesso dai log admin-tech. Per iniziare la valutazione di CVE-2026-20182, è necessario ricevere i file admin-tech da TUTTI i controller (vSmarts), validator (vBonds) e manager (vManage), inclusi tutti i nodi Manager (vManage) se in cluster.

Passaggi successivi:

Caricare i file admin-tech rimanenti non appena possibile.

Distinti saluti,

Apri in Outlook

① Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (con corpo)

⬇ Scarica modello .eml

TAC 1 - Indagine - Necessaria ulteriore revisione (sospetto IoC)

Scenario d'uso

Inviato da un tecnico TAC dopo che l'automazione ha individuato dei log che indicano possibili compromessi ed è richiesta un'indagine da parte dell'uomo.

Oggetto

N. RS - Ulteriori informazioni richieste

Messaggio

Gentile Cliente,

Il mio nome è {your_name} e ho accettato la tua richiesta. Grazie per la collaborazione con il Technical Assistance Center (TAC) di Cisco.

A seguito di un'analisi preliminare dei file admin-tech forniti dai **componenti di controllo SD-WAN**, abbiamo identificato che è necessaria un'ulteriore indagine TAC per completare la nostra analisi. Per contribuire a garantire una risoluzione accurata e completa, lavorerò in stretta collaborazione con voi per i prossimi passi.

Vi assicuriamo che ci impegniamo a supportarvi in queste fasi successive e forniremo una guida chiara per affrontare la situazione in modo efficace.

Impostare la pianificazione e l'esecuzione dell'aggiornamento come fase critica per ridurre questo rischio. Se l'aggiornamento non è stato ancora pianificato, procedere immediatamente.

In caso di dubbi o di necessità di assistenza, rivolgersi al tecnico TAC.

Grazie per l'attenzione e la collaborazione.

Distinti saluti,

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (con corpo)

↓ Scarica modello .eml

TAC 2 - Risultato - Nessun IoC trovato (confermato dal tecnico)

Scenario d'uso

Inviato dal tecnico TAC dopo che l'automazione non ha trovato alcun indicatore di compromissione e il tecnico ha confermato il risultato.

Oggetto

Messaggio

Salve [Nome cliente],

Sono il tecnico Cisco TAC assegnato al tuo caso [Numero SR].

Dopo aver eseguito una scansione preliminare dei file admin-tech forniti dai componenti di controllo SD-WAN, non sono state trovate voci di log coerenti con gli indicatori di compromesso descritti nei consigli di sicurezza di Cisco SD-WAN:

- **Vulnerabilità del bypass dell'autenticazione del controller SD-WAN Cisco Catalyst [1]**
- **Vulnerabilità di Cisco Catalyst SD-WAN Manager [2]**

Tuttavia, si dovrebbe procedere ad aggiornare tutti i componenti di controllo SD-WAN a <insert version>. Per procedere con l'aggiornamento, procedere come segue:

- **Avvio dell'aggiornamento di Catalyst SD-WAN [3]**
- **Guida all'aggiornamento di Cisco SD-WAN[4]**

Si noti che Cisco non è in grado di valutare i log dai dispositivi periferici a causa della natura dinamica degli indirizzi IP su Internet e della scarsa conoscenza degli indirizzi IP previsti dei dispositivi periferici nella rete del cliente. Per completare manualmente questo passaggio, i clienti sono invitati a seguire le linee guida sulla convalida degli eventi di peer indicate in Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability Security Advisory. I clienti sono inoltre invitati a completare le operazioni di rilevamento aggiuntive relative alla convalida degli eventi peer, come descritto nell'advisory della sicurezza per CVE-2026-20182.

Collegamenti

[1] Vulnerabilità del bypass di autenticazione del controller SD-WAN Cisco Catalyst -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Vulnerabilità di Cisco Catalyst SD-WAN Manager -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Avviare l'aggiornamento di Catalyst SD-WAN - <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Guida all'aggiornamento di Cisco SD-WAN - <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

Cordiali saluti,

Apri in Outlook

① Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

TAC 3 - Convalida - Conferma proprietà IP in sovrimpressione

Scenario d'uso

Inviato dal tecnico TAC per chiedere al cliente se gli indirizzi IP specifici rilevati durante l'analisi del log fanno o meno parte dell'infrastruttura di sovrimpressione SD-WAN.

Oggetto

[N. SR] - Convalida indirizzo IP richiesta

Messaggio

Gentile [Nome cliente],

Il mio nome è [Nome] e sono il tecnico Cisco TAC assegnato alla tua richiesta.

Come parte della nostra analisi continua dei file admin-tech forniti dai componenti di controllo SD-WAN, abbiamo bisogno del vostro aiuto per verificare se i seguenti indirizzi IP sono o sono stati in precedenza parte della vostra infrastruttura SD-WAN overlay:

Indirizzi IP in questione:

- [Indirizzo IP 1]
- [Indirizzo IP 2]

Per completare la valutazione, confermare:

1. Questo indirizzo IP è attualmente associato a qualsiasi componente nella sovrimpressione SD-WAN (ad esempio, vManage, vSmart, vBond o edge device)?
2. L'indirizzo IP è stato utilizzato in precedenza da qualsiasi componente di controllo SD-WAN che potrebbe essere stato disattivato o il cui IP è stato modificato?
3. Questo IP è associato a un sito di disaster recovery (DR) o a qualsiasi altra infrastruttura correlata all'installazione SD-WAN?

La tua risposta tempestiva ci consentirà di continuare la nostra analisi e di fornirti le fasi successive appropriate.

In caso di domande, non esiti a contattarci.

Distinti saluti,

Apri in Outlook

① Sostituire tutti i [segnaposto tra parentesi] prima dell'invio.

✉ Apri Outlook (con corpo)

📎 Scarica modello .eml

TAC 4 - Risultato - Falso positivo cancellato

Scenario d'uso

Inviato da un tecnico TAC dopo una revisione manuale determina che l'loC iniziale contrassegnato dalla scansione automatica è risultato un falso positivo.

Oggetto

Update: Riesame tecnico per CVE-2026-20182 - Caso [Numero caso]

Messaggio

Gentile Cliente,

Grazie per la pazienza dimostrata durante la revisione manuale dei file admin-tech forniti dai componenti di controllo SD-WAN da parte del team di progettazione.

A seguito di un'indagine approfondita, abbiamo stabilito che l'indicatore iniziale di compromesso (loC) contrassegnato dal nostro processo di scansione automatizzata era un falso positivo, cioè la nostra valutazione è che gli loC non sono validi.

Importante: Anche se questo avviso specifico è stato cancellato, si noti che la vulnerabilità associata a [CVE-2026-20182](#)^[1] richiede un aggiornamento del software per garantire la sicurezza e l'integrità a lungo termine del fabric SD-WAN.

Se l'aggiornamento non è stato ancora completato: Assegnate la priorità all'upgrade completo dei componenti di controllo SD-WAN non appena possibile. L'aggiornamento è l'unico modo per rimediare efficacemente a questa vulnerabilità. Per istruzioni dettagliate, consultare la [Guida all'aggiornamento di Cisco SD-WAN](#)^[2].

Se l'aggiornamento è già stato completato: Poiché questo risultato è stato confermato come falso positivo e l'utente ha già eseguito il monitoraggio e l'aggiornamento del software, non sono necessarie ulteriori azioni. È possibile considerare risolta questa controversia e procedere con le procedure di chiusura standard.

EMC apprezza la diligenza dimostrata nell'assegnare le priorità alla sicurezza dell'infrastruttura. Per ulteriori domande o per richiedere ulteriore assistenza, non esitate a contattarci.

Distinti saluti,
Cisco Technical Assistance Center (TAC)

Collegamenti:

[1] [Consulenza ufficiale sulla sicurezza](#)

[2] [Guida all'aggiornamento di Cisco SD-WAN](#)

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

TAC 5 - Critico - Identificato IoC, pianifica chiamata di revisione

Scenario d'uso

Inviato dal tecnico TAC quando sono stati confermati potenziali indicatori di compromissione ed è necessaria una chiamata urgente del cliente per discutere i risultati e le fasi successive.

Oggetto

URGENTE: Risultati dell'analisi per CVE-2026-20182 - Indicatore di compromesso identificato

Messaggio

Gentile Cliente,

Grazie per la pazienza dimostrata durante l'analisi dei file admin-tech forniti per i componenti di controllo SD-WAN.

A seguito della nostra revisione tecnica, abbiamo identificato potenziali indicatori di compromesso (IoC) relativi a CVE-2026-20182.

Data la natura di questi risultati, è fondamentale discutere quanto prima i dettagli tecnici e le fasi successive raccomandate. Vorremmo chiamare il tuo team per esaminare i risultati specifici e discutere le soluzioni appropriate.

Passaggi successivi:

- **Pianifica riunione:** Comunicaci la tua disponibilità per una breve chiamata entro le prossime [ad es., 4-8 ore] per

rivedere i risultati.

- **Aggiornamento dei componenti di controllo SDWAN:** Aggiornare SDWAN Manager, Controller e Validator a una versione fissa il prima possibile.

L'obiettivo principale di EMC è quello di aiutare le aziende a proteggere l'ambiente e a ridurre i potenziali rischi. Appreziamo la tua sollecita attenzione su questa questione e ci auguriamo di stabilire un coordinamento con te.

Distinti saluti,

Apri in Outlook

① Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (con corpo)

↓ Scarica modello .eml

TAC 6 - Risultato - IoC duplicato (Close & Redirect)

Scenario d'uso

Inviato dal tecnico TAC quando l'analisi IoC conferma risultati che corrispondono a una SR precedente per lo stesso cliente/ambiente. Il caso in corso è chiuso e il cliente viene reindirizzato alla SR originale in cui sono già state fornite le linee guida per la risoluzione del problema.

Oggetto

Update: Revisione tecnica per CVE-2026-20182 - Caso [SR #] (IoC duplicato confermato)

Messaggio

Gentile Cliente,

Grazie per la pazienza dimostrata durante l'analisi dei file admin-tech forniti per i componenti di controllo SD-WAN. Abbiamo determinato che gli indicatori iniziali di compromissione (IoC) contrassegnati dal processo di scansione sono gli stessi già comunicati in **[Original SR #]**. Come già accennato, si consiglia di eseguire con urgenza un aggiornamento e di procedere con uno dei due percorsi di ripristino descritti nella [TAC Remediation Guide](#)^[2] per proteggere l'ambiente il più rapidamente possibile. Fare riferimento all'[advisory ufficiale della sicurezza per CVE-2026-20182](#)^[1] per informazioni dettagliate.

Ora chiuderò il caso. Utilizzare **[Original SR #]** per richiedere ulteriori informazioni o supporto tecnico in merito all'aggiornamento o alla risoluzione del problema.

Distinti saluti,
[Nome]

Collegamenti:

[1] [Consulenza ufficiale sulla sicurezza](#)

[2] [Guida alla correzione del TAC](#)

Apri in Outlook

❗ Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (con corpo)

⬇ Scarica modello .eml

TAC 7 - Rimedio - Opzioni - Seguito (dopo la chiamata)

Scenario d'uso

Inviato dopo la chiamata di revisione di IoC per riepilogare i percorsi di risoluzione discussi. Il cliente sceglie l'opzione A (Reinstallazione con riavvio in sequenza), l'opzione B (Reinstallazione con sostituzione hardware) o l'opzione C (Ricostruzione completa del sistema).

Oggetto

Follow-up: Opzioni di correzione per CVE-2026-20182

Messaggio

Gentile Cliente,

Grazie per il tempo dedicato alla discussione dei risultati della nostra recente analisi. Come descritto nella chiamata precedente, si consiglia di procedere con uno dei seguenti percorsi di ripristino per proteggere l'ambiente.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la

connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la ridistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti del controller precedenti vengono isolati dal nuovo fabric durante la ridistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione lunga e richiede l'esperienza necessaria per ricostruire i modelli e i database delle regole.

Passaggi successivi:

- Per favore, discutete queste opzioni internamente e fateci sapere quale strada intendete prendere. Una volta deciso, possiamo fornire ulteriore guida o supporto tecnico per assistervi nella fase di esecuzione.

Siamo qui per aiutarvi in questo processo. In caso di domande su queste opzioni, contattaci.

Distinti saluti,

Cisco Technical Assistance Center (TAC)

NOTA: L'opzione 1 era l'aggiornamento. Lo scenario considerato ha già eseguito l'aggiornamento.

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

📎 Scarica modello .eml

TAC 8 - Risanamento - Opzioni aggiornate per i fabric compromessi (opzione 2 follow-up)

Scenario d'uso

Per notificare i clienti i cui fabric SD-WAN sono stati compromessi e precedentemente perseguiti con l'opzione 2 e i cui fabric sono ritenuti ancora a rischio di persistenza dell'attore di minaccia. I clienti che hanno ricostruito il fabric compromesso (e non si sono affidati a un configDB di backup/esistente) non sono considerati a rischio e non riceveranno questa comunicazione. La comunicazione sarà inviata entro il giorno lavorativo successivo.

Oggetto

Necessità Di Un'Azione Urgente: Risanamento delle vulnerabilità critiche dell'infrastruttura SD-WAN

Messaggio

Gentile Cliente,

Viene fornito un aggiornamento critico per il ripristino del fabric SD-WAN, come indicato in [SR#] e negli avvisi sulla sicurezza comunicati in precedenza. Questo aggiornamento è specifico per i fabric in cui i log forniti mostravano evidenze di indicatori di compromissione (IOC).

Anche se in precedenza è stato selezionato un piano di risanamento basato sull'opzione 2, che prevede l'aggiornamento del software, la reinstallazione dei controller e la rotazione delle chiavi SSH, l'analisi delle minacce continua a evolversi. Nuove conoscenze tecniche relative allo sfruttamento di queste vulnerabilità indicano che è vivamente necessario adottare misure supplementari per ridurre il rischio di persistenza e contribuire a garantire l'integrità della catena di certificati.

AZIONE RICHIESTA:

Le strategie di correzione consigliate sono state aggiornate per fornire una difesa più completa, includendo una rotazione aggiuntiva dei certificati radice.

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete.

Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la ridistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti del controller precedenti vengono isolati dal nuovo fabric durante la ridistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione lunga e richiede l'esperienza necessaria per ricostruire i

modelli e i database delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Appreziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, è possibile aprire una richiesta di assistenza (SR) presso il Technical Assistance Center (TAC).

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

TAC 17 - Risultato inverso - In precedenza non esisteva IoC, ora IoC identificato (CVE-2026-20182)

Scenario d'uso

Inviato a clienti **precedentemente informati che non** sono stati trovati **indicatori di compromissione (IoC)**, ma per i quali una **successiva revisione interna** dei registri admin-tech ha **identificato gli IoC** relativi a CVE-2026-20182. Comunica il risultato rivisto e fornisce le tre opzioni di correzione (opzione A, B o C).

Oggetto

Aggiornamento importante: Valutazione dell'IoC rivista per CVE-2026-20182 - Indicatori di compromessi ora identificati - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per la collaborazione con il Cisco Technical Assistance Center (TAC) relativamente a CVE-2026-20182 in base alla richiesta di assistenza [SR#].

Nella nostra corrispondenza precedente, abbiamo avvisato che la nostra analisi dei file admin-tech forniti dai vostri componenti di controllo SD-WAN non ha identificato alcun Indicator of Compromise (IoC) relativo a questo avviso. Come parte del nostro continuo impegno per la sicurezza dei clienti, da allora abbiamo eseguito una revisione interna di routine

di ulteriori dati di log admin-tech associati al fabric dell'organizzazione.

Questo riesame successivo ha individuato gli indicatori di compromesso (IoC) che non sono stati messi in evidenza durante la valutazione iniziale. Stiamo ora collaborando con voi per risolvere questi problemi. Questi IoC indicano attività potenzialmente sospette all'interno della struttura dell'organizzazione che richiedono azioni correttive.

In questo modo vengono rivisti i risultati comunicati in precedenza e si vuole essere certi che il cliente disponga di un'immagine chiara e accurata dell'ambiente in modo da poter adottare le misure correttive appropriate.

AZIONE RICHIESTA:

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete.

Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la ridistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti del controller precedenti vengono isolati dal nuovo fabric durante la ridistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione che richiede una notevole esperienza nella ricostruzione dei database dei modelli e delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Apprezziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti

tecnici, rispondete a questa e-mail o inviate una richiesta di assistenza (SR) con il nostro Technical Assistance Center (TAC).

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

CloudOps 1 - Proattivo - Rilevato IoC nella scansione del cloud, richiesto Admin-Tech per la convalida

Scenario d'uso

Inviato in modo proattivo quando un'analisi della sicurezza Cisco CloudOps di un fabric SD-WAN ospitato nel cloud ha individuato potenziali indicatori di compromesso (IoC). Viene aperta una SR per conto del cliente, che deve allegare i file admin-tech in modo che il risultato possa essere convalidato attraverso l'analisi completa del log.

Oggetto

Azione richiesta: File admin-tech necessari per convalidare i risultati dell'analisi di protezione - SR [SR#]

Messaggio

Gentile Cliente,

Nell'ambito del nostro continuo impegno per la sicurezza e il monitoraggio dell'integrità delle offerte Cisco, Cisco ha recentemente completato una scansione di sicurezza di alcuni fabric SD-WAN ospitati su cloud. Questa azione è stata intrapresa in risposta a un problema di sicurezza segnalato. L'analisi ha identificato attività potenzialmente sospette nella struttura dell'organizzazione che richiedono un ulteriore esame.

Le chiediamo di fornirle assistenza per allegare file admin-tech a questa richiesta di assistenza (SR), che è stata aperta per suo conto, in modo che possiamo convalidare questo risultato e completare l'indagine.

Per abilitare un'analisi completa, raccogliere e caricare i file admin-tech da tutti i componenti di controllo SD-WAN. Accertarsi di selezionare sia **"Log"** che **"Tech"** durante la generazione di questi file:

- **Smarts (controller):** Raccoglierne uno alla volta, non contemporaneamente.

- **vBonds (validatori):** Raccogli da tutti i nodi.
- **Manager (vManage):** Eseguire la raccolta da tutti i nodi nel cluster (DR attivo e in standby).

Per istruzioni dettagliate su come generare e inviare in modo sicuro i file admin-tech, fare riferimento a questa guida:

[Cisco SD-WAN Admin-Tech Collection Guide](#)^[1].

Una volta ricevuti i file richiesti, il nostro team li analizzerà per confermare se l'attività osservata rappresenta un autentico indicatore di compromissione e vi consiglierà sulle fasi successive appropriate.

Appreziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, è possibile rispondere a questa richiesta di assistenza (SR).

Distinti saluti,

Cisco

Collegamenti:

[1] [Guida alla raccolta di Cisco SD-WAN Admin-Tech](#)

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Messaggi di posta elettronica per la WAVE 2A per clienti precedentemente interessati che non hanno ancora completato le opzioni A, B o C. (È necessario ripetere le opzioni 1 e 2)

Modello TAC 9 senza COI per PSIRT2a/sono stati ricostruiti (**precedentemente interessati**)

Scenario d'uso

Inviato a clienti i cui log SD-WAN **non** mostravano **alcun Indicator of Compromise (IoC)** correlato all'advisory PSIRT2a E che **precedentemente** hanno **ricostruito** il fabric. Fornisce una guida aggiornata alla risoluzione dei problemi con tre opzioni (follow-up dell'opzione 2).

Oggetto

Necessità Di Un'Azione Urgente: Risoluzione dei problemi di vulnerabilità critici dell'infrastruttura SD-WAN - SR [SR#]

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) riguardo i recenti consigli PSIRT SD-WAN in Service Request [SR#].

Dopo aver esaminato i log e le informazioni fornite dal vostro fabric SD-WAN, la nostra analisi non ha identificato alcun Indicator of Compromise (IOC) associato al 5 giugno 2026 SD-WAN vulnerability advisory. Inoltre, è noto che l'ambiente è stato precedentemente ricostruito nell'ambito delle attività di correzione correlate ai consigli precedenti.

Desideriamo condividere un importante aggiornamento relativo alle linee guida per la correzione consigliate per i fabric SD-WAN, tenendo conto delle nuove informazioni identificate relative a queste vulnerabilità.

Viene fornito un aggiornamento critico per il ripristino del fabric SD-WAN, come indicato in [SR#] e negli avvisi sulla sicurezza comunicati in precedenza.

Anche se in precedenza è stato selezionato un piano di risanamento basato sull'opzione 2, che prevede l'aggiornamento del software, la reinstallazione dei controller e la rotazione delle chiavi SSH, l'analisi delle minacce continua a evolversi. Nuove conoscenze tecniche relative allo sfruttamento di queste vulnerabilità indicano che è vivamente necessario adottare misure supplementari per ridurre il rischio di persistenza e contribuire a garantire l'integrità della catena di certificati.

AZIONE RICHIESTA:

Le strategie di correzione consigliate sono state aggiornate per fornire una difesa più completa, includendo una rotazione aggiuntiva dei certificati radice.

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete. Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il

tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la ridistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti del controller precedenti vengono isolati dal nuovo fabric durante la ridistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione che richiede una notevole esperienza nella ricostruzione dei database dei modelli e delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Appreziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, rispondete a questa e-mail o tramite la richiesta di assistenza esistente.

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Modello TAC 10 per sì IOC per PSIRT2a/sono stati ricostruiti (**precedentemente interessati**)

Scenario d'uso

Inviato a clienti i cui log SD-WAN mostravano **Indicators of Compromise (IoCs)** relativi all'advisory PSIRT2a E che **precedentemente** hanno **ricostruito** il fabric. Fornisce una guida aggiornata alla risoluzione dei problemi con tre opzioni (follow-up dell'opzione 2).

Oggetto

Necessità Di Un'Azione Urgente: Risoluzione dei problemi di vulnerabilità critici dell'infrastruttura SD-WAN - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) riguardo i recenti consigli PSIRT SD-WAN in Service Request [SR#].

Dopo aver analizzato i log forniti dal fabric SD-WAN, il nostro team ha identificato gli Indicatori di Compromesso (IOC) associati all'advisory della vulnerabilità SD-WAN del 5 giugno 2026. È inoltre noto che l'ambiente è stato precedentemente sottoposto a una ricostruzione come parte delle operazioni di ripristino relative ai consigli precedenti.

Viene fornito un aggiornamento critico per il ripristino del fabric SD-WAN, come indicato in [SR#] e negli avvisi sulla sicurezza comunicati in precedenza. Questo aggiornamento è specifico per i fabric in cui i log forniti mostravano evidenze di indicatori di compromissione (IOC).

Anche se in precedenza è stato selezionato un piano di risanamento basato sull'opzione 2, che prevede l'aggiornamento del software, la reinstallazione dei controller e la rotazione delle chiavi SSH, l'analisi delle minacce continua a evolversi. Nuove conoscenze tecniche relative allo sfruttamento di queste vulnerabilità indicano che è vivamente necessario adottare misure supplementari per ridurre il rischio di persistenza e contribuire a garantire l'integrità della catena di certificati.

AZIONE RICHIESTA:

Le strategie di correzione consigliate sono state aggiornate per fornire una difesa più completa, includendo una rotazione aggiuntiva dei certificati radice.

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete. Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la redistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti del controller precedenti vengono isolati dal nuovo fabric durante la redistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione che richiede una notevole esperienza nella ricostruzione dei database dei modelli e delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Apprezziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, rispondete a questa e-mail o tramite la richiesta di assistenza esistente.

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Modello TAC 11 per nessun COI per PSIRT2a/non sono stati ricostruiti (precedentemente interessati)

Scenario d'uso

Inviato a clienti i cui log SD-WAN **non** mostravano **alcun Indicator of Compromise (IoC)** relativo all'advisory PSIRT2a E che **NON** hanno **ricostruito** il fabric. Fornisce una guida aggiornata alla risoluzione dei problemi con tre opzioni (opzione 1 follow-up).

Oggetto

Necessità Di Un'Azione Urgente: Risoluzione dei problemi di vulnerabilità critici dell'infrastruttura SD-WAN - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) riguardo i recenti consigli PSIRT SD-WAN in

Service Request [SR#].

Dopo aver esaminato i registri e le informazioni fornite dal fabric SD-WAN, non abbiamo identificato gli Indicatori di Compromesso (IOC) associati all'advisory della vulnerabilità SD-WAN del 5 giugno 2026.

Sappiamo anche che l'ambiente non è stato completamente ricostruito in base ai consigli precedenti. Cisco consiglia di rivedere le linee guida per la risoluzione dei problemi aggiornate riportate di seguito per ridurre l'esposizione potenziale e rafforzare l'integrità della catena di certificati SD-WAN.

Tenendo presente questo aspetto, forniamo un aggiornamento critico per il ripristino del fabric SD-WAN, come indicato in [SR#] e negli avvisi sulla sicurezza comunicati in precedenza.

Anche se in precedenza è stato selezionato un piano di risanamento basato sull'opzione 1, che include un aggiornamento del software e la rotazione della chiave SSH, l'analisi del panorama delle minacce continua a evolversi. Nuove conoscenze tecniche relative allo sfruttamento di queste vulnerabilità indicano che è vivamente necessario adottare misure supplementari per ridurre il rischio di persistenza e contribuire a garantire l'integrità della catena di certificati.

AZIONE RICHIESTA:

Le strategie di correzione consigliate sono state aggiornate per fornire una difesa più completa, includendo una rotazione aggiuntiva dei certificati radice.

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete. Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la ridistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la ridistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti

del controller precedenti vengono isolati dal nuovo fabric durante la redistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione che richiede una notevole esperienza nella ricostruzione dei database dei modelli e delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Appreziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, rispondete a questa e-mail o tramite la richiesta di assistenza esistente.

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i *[segnaposto tra parentesi]* prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Modello TAC 12 per sì IOC per PSIRT2a/non sono stati ricostruiti (**precedentemente interessati**)

Scenario d'uso

Inviato a clienti i cui log SD-WAN mostravano **Indicators of Compromise (IoCs)** relativi all'advisory PSIRT2a E che **NON hanno ricostruito** il fabric. Fornisce una guida aggiornata alla risoluzione dei problemi con tre opzioni (opzione 1 follow-up).

Oggetto

Necessità Di Un'Azione Urgente: Risoluzione dei problemi di vulnerabilità critici dell'infrastruttura SD-WAN - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) riguardo i recenti consigli PSIRT SD-WAN in Service Request [SR#].

Dopo aver analizzato i log forniti dal fabric SD-WAN, il nostro team ha identificato gli Indicatori di Compromesso (IOC) associati all'advisory della vulnerabilità SD-WAN del 5 giugno 2026. Inoltre, siamo consapevoli che l'ambiente non è stato completamente ricostruito in base ai precedenti consigli.

Data la presenza di questi indicatori e la comprensione in continua evoluzione del panorama delle minacce, è importante rivedere e implementare le linee guida aggiornate per la risoluzione dei problemi descritte di seguito per ridurre il rischio di persistenza e garantire l'integrità della catena di certificati SD-WAN.

Viene fornito un aggiornamento critico per il ripristino del fabric SD-WAN, come indicato in [SR#] e negli avvisi sulla sicurezza comunicati in precedenza. Questo aggiornamento è specifico per i fabric in cui i log forniti mostravano evidenze di indicatori di compromissione (IOC).

Anche se in precedenza è stato selezionato un piano di risanamento basato sull'opzione 1, che include un aggiornamento del software e la rotazione della chiave SSH, l'analisi del panorama delle minacce continua a evolversi. Nuove conoscenze tecniche relative allo sfruttamento di queste vulnerabilità indicano che è vivamente necessario adottare misure supplementari per ridurre il rischio di persistenza e contribuire a garantire l'integrità della catena di certificati.

AZIONE RICHIESTA:

Le strategie di correzione consigliate sono state aggiornate per fornire una difesa più completa, includendo una rotazione aggiuntiva dei certificati radice.

Si tenga presente che gli interventi correttivi richiederanno attività di manutenzione aggiuntive, che possono includere tempi di inattività pianificati per la rete. Poiché la nostra priorità è la sicurezza e l'integrità della rete, abbiamo sviluppato tre diverse opzioni di ripristino. Ciascuna delle opzioni riportate di seguito rappresenta un compromesso tra l'impatto operativo e la sicurezza. Poiché la postura del rischio interno è univoca, Cisco non può consigliare un percorso particolare.

Opzione A. Ridistribuzione con riavvio in sequenza. Assegna priorità alla continuità operativa evitando i tempi di inattività della rete, sebbene comporti un rischio residuo di persistenza delle minacce durante il processo di transizione.

Descrizione: Prevede la redistribuzione del controller, oltre alla rotazione della chiave SSH e del certificato. Durante la migrazione tramite vManage, i componenti del controller esistenti vengono connessi per distribuire la nuova struttura. Ogni componente viene quindi rimosso non appena viene eseguita la migrazione del dispositivo.

Opzione B. Reinstallazione con hard cutover. Fornisce un livello più elevato di sicurezza. Poiché i nuovi controller non si connettono mai ai vecchi controller, esiste un isolamento completo. Questo influisce sulle operazioni complessive della rete, in quanto tutti i dispositivi devono ristabilire la connettività e scambiare le informazioni sulla route e la connettività. Il tempo di interruzione dipenderà dal numero di siti, dal numero di prefissi scambiati e così via.

Descrizione: Prevede la redistribuzione del controller più la rotazione della chiave SSH e del certificato, ma i componenti

del controller precedenti vengono isolati dal nuovo fabric durante la redistribuzione.

Opzione C: Ricostruzione completa del sistema. Fornisce il massimo livello di sicurezza stabilendo una linea di base pulita, anche se si tratta dell'approccio più complesso e comporta un rischio maggiore di instabilità relativa alla configurazione durante la ricostruzione. Si tratta di un'opzione che richiede una notevole esperienza nella ricostruzione dei database dei modelli e delle regole.

Dopo che il team ha esaminato queste opzioni e ha identificato l'approccio che meglio si allinea agli standard di gestione dei rischi, è possibile rispondere a questo messaggio. Una volta ricevuta la selezione, coordineremo la finestra di manutenzione e inizieremo i preparativi tecnici necessari per l'esecuzione.

Appreziamo l'impegno costante dell'azienda nel mantenimento di un'infrastruttura di rete sicura. Per ulteriori chiarimenti tecnici, rispondete a questa e-mail o tramite la richiesta di assistenza esistente.

Cordiali saluti,
Cisco

Apri in Outlook

① Utilizzare il download .eml riportato di seguito. Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

E-mail per WAVE 2A per NUOVI clienti (nessun impatto precedente)

Modello TAC 13 per senza IOC/senza versione fissa disponibile (WAVE 2a — Await Fix)

Scenario d'uso

Inviato a clienti i cui log SD-WAN **non** mostravano **alcun Indicator of Compromise (IoC)** relativo a CVE-2026-20245, ma per i quali **non è attualmente disponibile una versione software fissa** per la piattaforma/versione. Consiglia al cliente di applicare misure provvisorie di protezione avanzata e di attendere la notifica di rilascio fisso.

Oggetto

Update: Valutazione IoC completata per CVE-2026-20245 - Nessuna versione fissa attualmente disponibile - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) per quanto riguarda CVE-2026-20245 in base alla richiesta di assistenza [SR#].

Abbiamo completato l'analisi dei file admin-tech forniti dai componenti di controllo SD-WAN. **Nei registri esaminati non sono stati identificati indicatori di compromesso** associati a CVE-2026-20245.

La quantità di dati di log recuperati e forniti a Cisco per questa revisione potrebbe essere stata limitata dal periodo di conservazione dei log configurato nell'ambiente in uso in base alla [Cisco SD-WAN Hardening Guide](#)^[1].

Importante — Non è attualmente disponibile una versione software fissa:

Al momento, **non è disponibile alcuna versione software fissa** per la piattaforma e la versione software correnti per correggere questa vulnerabilità. Il team di progettazione Cisco sta lavorando attivamente per fornire una release fissa. Una volta reso disponibile il software fisso, l'[advisory ufficiale della sicurezza](#)^[2] verrà aggiornato con le informazioni sulla versione fissa.

Azioni provvisorie consigliate:

In attesa del rilascio fisso, si consiglia di implementare le seguenti misure di protezione avanzata per ridurre l'esposizione:

1. **Applica procedure ottimali di protezione avanzata:** Esaminare e implementare le raccomandazioni contenute nella [Cisco SD-WAN Hardening Guide](#)^[1] per ridurre la superficie di attacco.
2. **Monitorare l'advisory della sicurezza:** Consultare periodicamente l'[advisory ufficiale della sicurezza](#)^[2] per gli aggiornamenti sulla disponibilità di versioni fisse per la piattaforma.
3. **Pianificazione aggiornamento:** Iniziare subito la pianificazione dell'aggiornamento in modo da essere pronti a eseguire l'aggiornamento immediatamente dopo la pubblicazione della versione fissa.
4. **Monitoraggio dell'ambiente:** Continuare a monitorare i componenti di controllo SD-WAN per rilevare eventuali comportamenti anomali o modifiche impreviste alla configurazione.

Passaggi successivi:

Il caso verrà aggiornato quando sarà disponibile la versione software fissa. A quel punto, si dovrebbe dare priorità all'aggiornamento di tutti i componenti di controllo SD-WAN (Manager, Controller, Validator) alla versione fissa non appena possibile.

Se disponi di un abbonamento BCS/LCS, contatta il tuo Cisco NCE o il tuo Delivery Manager per ricevere ulteriore assistenza sulla pianificazione dell'aggiornamento.

Grazie per la pazienza e l'impegno dimostrato verso la sicurezza dell'infrastruttura. In caso di domande o di ulteriore assistenza nel frattempo, non esiti a rispondere a questo caso.

Distinti saluti,
Cisco Technical Assistance Center (TAC)

Collegamenti:

[1] [Guida alla protezione avanzata di Cisco SD-WAN](#)

[2] [Consulenza ufficiale sulla sicurezza \(cisco-sa-sdwan-privesc-4uxFrzx\)](#)

Apri in Outlook

❗ Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Modello TAC 14 per rilascio fisso non disponibile (WAVE 2a — Aggiorna ora)

Scenario d'uso

Inviato a clienti i cui log SD-WAN **non** mostravano **Indicatori di Compromesso (IoC)** relativi a CVE-2026-20245 E per i quali è **disponibile** una **versione software fissa**. Consiglia al cliente di procedere immediatamente con la pianificazione e l'esecuzione dell'aggiornamento.

Oggetto

Update: Valutazione IoC completata per CVE-2026-20245 - Nessun IoC trovato, aggiornamento richiesto - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) per quanto riguarda CVE-2026-20245 in base alla richiesta di assistenza [SR#].

Abbiamo completato l'analisi dei file admin-tech forniti dai componenti di controllo SD-WAN. **Nei** registri esaminati **non sono stati identificati indicatori di compromesso** associati a CVE-2026-20245.

La quantità di dati di log recuperati e forniti a Cisco per questa revisione potrebbe essere stata limitata dal periodo di conservazione dei log configurato nell'ambiente in uso in base alla [Cisco SD-WAN Hardening Guide](#)^[1].

Importante — Aggiornamento richiesto:

Sebbene non siano stati identificati IoC, la vulnerabilità sottostante rimane presente finché i componenti di controllo SD-WAN non vengono aggiornati a una versione software fissa. È ora disponibile una versione fissa per la piattaforma in uso.

Assegnare la **priorità alla pianificazione e all'esecuzione dell'aggiornamento** come fase più critica per correggere questa vulnerabilità. Se l'aggiornamento non è stato ancora pianificato, procedere immediatamente.

Passaggi successivi:

1. **Upgrade di tutti i componenti di controllo SD-WAN:** Aggiornare Manager (vManage), Controller (vSmart) e Validator (vBond) a una versione software fissa elencata nell'[advisory ufficiale della sicurezza](#)^[2].
2. **Risorse di aggiornamento:** Per istruzioni dettagliate sull'aggiornamento, consultare i seguenti documenti ufficiali di Cisco:
 - [Avvio dell'aggiornamento di Catalyst SD-WAN](#)^[3]
 - [Guida all'aggiornamento di Cisco SD-WAN](#)^[4]
3. **Chiusura della richiesta:** Una volta completato l'aggiornamento del software nell'ambiente, è possibile prendere in considerazione la risoluzione del caso e procedere con le procedure di chiusura standard.

Se disponi di un abbonamento BCS/LCS, contatta il tuo Cisco NCE o il tuo Delivery Manager per ricevere ulteriori informazioni sul processo di aggiornamento.

Continueremo a monitorare il tuo caso. Se non riceviamo risposta entro 10 giorni lavorativi, presumiamo che non sia necessaria ulteriore assistenza e procediamo con le normali procedure di chiusura dei casi TAC.

Distinti saluti,
Cisco Technical Assistance Center (TAC)

Collegamenti:

- [1] [Guida alla protezione avanzata di Cisco SD-WAN](#)
- [2] [Consulenza ufficiale sulla sicurezza \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [3] [Avviare l'aggiornamento di Catalyst SD-WAN](#)
- [4] [Guida all'aggiornamento di Cisco SD-WAN](#)

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Urgent Upgrade)

Scenario d'uso

Inviato a clienti i cui log SD-WAN mostravano **Indicatori di Compromesso (IoC)** relativi a CVE-2026-20245 E per i quali è **disponibile una versione software fissa**. Consiglia al cliente di eseguire l'aggiornamento con urgenza e di pianificare una chiamata di revisione per discutere i risultati e le azioni correttive.

Oggetto

URGENTE: IoC identificato per CVE-2026-20245 - Aggiornamento immediato richiesto - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) per quanto riguarda CVE-2026-20245 in base alla richiesta di assistenza [SR#].

Dopo aver analizzato i file admin-tech forniti dai componenti di controllo SD-WAN, il nostro team ha **identificato gli Indicatori di Compromesso (IoC)** associati a CVE-2026-20245.

Data la natura di questi risultati, è fondamentale discutere quanto prima i dettagli tecnici e le fasi successive raccomandate. Si desidera pianificare una chiamata con il team del cliente per esaminare i risultati specifici e discutere il percorso di risoluzione appropriato.

Azioni immediate richieste:

- 1. Aggiornamento immediato dei componenti di controllo SD-WAN:** È disponibile una versione software fissa per la piattaforma. Aggiornare appena possibile Manager (vManage), Controller (vSmart) e Validator (vBond) a una versione software fissa elencata nell'[advisory ufficiale della sicurezza](#)^[1]. L'aggiornamento chiude immediatamente la vulnerabilità.
- 2. Pianifica una chiamata di revisione:** Comunicaci la tua disponibilità per una breve chiamata entro le prossime [ad esempio, 4-8 ore] per rivedere i risultati dell'IoC e discutere le opzioni di risanamento consigliate.
- 3. Applica procedure ottimali di protezione avanzata:** Esaminare e implementare i suggerimenti contenuti nella [Cisco SD-WAN Hardening Guide](#)^[2] per ridurre la superficie di attacco durante la pianificazione della risoluzione.

Risorse di aggiornamento:

- [Avvio dell'aggiornamento di Catalyst SD-WAN](#)^[3]
- [Guida all'aggiornamento di Cisco SD-WAN](#)^[4]

Importante: In seguito all'aggiornamento, possono essere consigliati ulteriori passaggi di risoluzione del problema (ad esempio la redistribuzione del controller e la rotazione dei certificati) a seconda della gravità del problema identificato. Tali

questioni saranno discusse durante il bando di revisione.

Per informazioni dettagliate sulle opzioni di ripristino, consultare la [Guida](#) alle misure correttive del TAC^[5].

L'obiettivo principale di EMC è quello di aiutare le aziende a proteggere l'ambiente e a ridurre i potenziali rischi. Apprezziamo la tua sollecita attenzione su questa questione e ci auguriamo di stabilire un coordinamento con te.

Distinti saluti,
Cisco Technical Assistance Center (TAC)

Collegamenti:

- [1] [Consulenza ufficiale sulla sicurezza \(cisco-sa-sdwan-privesc-4uxFrzx\)](#)
- [2] [Guida alla protezione avanzata di Cisco SD-WAN](#)
- [3] [Avviare l'aggiornamento di Catalyst SD-WAN](#)
- [4] [Guida all'aggiornamento di Cisco SD-WAN](#)
- [5] [Guida alla correzione del TAC](#)

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

Modello TAC 16 per IOC identificato / non è disponibile alcuna versione fissa (WAVE 2a — Harden & Await Fix)

Scenario d'uso

Inviato a clienti i cui log SD-WAN mostravano **Indicatori di Compromesso (IoC)** relativi a CVE-2026-20245, ma per i quali **non è attualmente disponibile una versione software fissa** per la piattaforma/versione. Consiglia la protezione avanzata immediata, pianifica una chiamata di revisione e informa il cliente che deve attendere che il rilascio fisso venga corretto completamente.

Oggetto

URGENTE: IoC identificato per CVE-2026-20245 - Nessuna versione fissa attualmente disponibile - SR [SR#]

Messaggio

Gentile Cliente,

Grazie per aver contattato il Cisco Technical Assistance Center (TAC) per quanto riguarda CVE-2026-20245 in base alla

richiesta di assistenza [SR#].

Dopo aver analizzato i file admin-tech forniti dai componenti di controllo SD-WAN, il nostro team ha **identificato gli Indicatori di Compromesso (IoC)** associati a CVE-2026-20245.

Data la gravità di questi risultati, è fondamentale discutere i dettagli tecnici e raccomandare azioni intermedie il più presto possibile. Desideriamo chiamare il tuo team per esaminare i risultati specifici.

Importante — Non è attualmente disponibile una versione software fissa:

Al momento, **non è disponibile alcuna versione software fissa** per la piattaforma e la versione software correnti per correggere completamente questa vulnerabilità. Il team di progettazione Cisco sta lavorando attivamente per fornire una release fissa. Una volta reso disponibile il software fisso, l'[advisory ufficiale della sicurezza](#)^[1] verrà aggiornato con le informazioni sulla versione fissa.

Azioni immediate richieste:

1. **Pianifica una chiamata di revisione:** Comunicaci la tua disponibilità per una breve telefonata entro le prossime [ad es., 4-8 ore] per esaminare i risultati dell'IoC e discutere le misure provvisorie di contenimento.
2. **Applicazione immediata delle procedure ottimali di protezione avanzata:** Esaminare e implementare i suggerimenti contenuti nella [Cisco SD-WAN Hardening Guide](#)^[2] per ridurre la superficie di attacco in attesa della versione fissa.
3. **Monitoraggio avanzato:** Monitorare attentamente i componenti di controllo SD-WAN per rilevare eventuali comportamenti anomali, modifiche impreviste alla configurazione o tentativi di accesso non autorizzati.
4. **Monitorare l'advisory della sicurezza:** Consultare periodicamente l'[advisory ufficiale della sicurezza](#)^[1] per gli aggiornamenti sulla disponibilità di versioni fisse per la piattaforma.
5. **Pianificazione aggiornamento:** Iniziare subito la pianificazione dell'aggiornamento in modo da essere pronti a eseguire l'aggiornamento immediatamente dopo la pubblicazione della versione fissa.

Passaggi successivi:

Il caso verrà aggiornato quando sarà disponibile la versione software fissa. A quel punto, è necessario dare priorità all'aggiornamento di tutti i componenti di controllo SD-WAN (Manager, Controller, Validator) alla versione fissa immediatamente. A seguito dell'aggiornamento, verranno illustrati ulteriori passaggi di risoluzione (come la reinstallazione del controller e la rotazione dei certificati) in base ai risultati esaminati durante la chiamata.

Fare riferimento anche alla [TAC Remediation Guide](#)^[3] per informazioni sulle opzioni di correzione che si applicheranno quando la versione fissa sarà disponibile.

L'obiettivo principale di EMC è quello di aiutare le aziende a proteggere l'ambiente e a ridurre i potenziali rischi.

Appreziamo la tua sollecita attenzione su questa questione e ci auguriamo di stabilire un coordinamento con te.

Distinti saluti,

Cisco Technical Assistance Center (TAC)

Collegamenti:

[1] [Consulenza ufficiale sulla sicurezza \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Guida alla protezione avanzata di Cisco SD-WAN](#)

[3] [Guida alla correzione del TAC](#)

Apri in Outlook

① Sostituire tutti i **[segnaposto tra parentesi]** prima dell'invio.

✉ Apri Outlook (solo oggetto)

↓ Scarica modello .eml

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).