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

Sommario

Introduzione

Questo documento descrive i passaggi per identificare e correggere le vulnerabilità critiche della sicurezza in SD-WAN in base agli advisory PSIRT del 14 maggio 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 del bypass dell'autenticazione del controller SD-WAN Cisco Catalyst
- Vulnerabilità di Cisco Catalyst SD-WAN

I seguenti problemi sono risolti dai consigli PSIRT:

- ID bug Cisco CSCwt50498
- ID bug Cisco CSCwt38739
- ID bug Cisco CSCwt38767
- ID bug Cisco CSCwt5544

Panoramica sul flusso di lavoro di risoluzione

Nota: Tutti i controller e i manager SD-WAN sono vulnerabili e richiedono un aggiornamento immediato per tutti i componenti di controllo. Tuttavia, non tutti i controller mostrano segni di compromissione.

Azione richiesta: Raccogliere dati tecnici da un amministratore, eseguire l'aggiornamento a una versione fissa e aprire una richiesta TAC per Cisco, in modo che TAC possa analizzare i dati tecnici dall'amministratore e individuare eventuali indicatori di compromesso.

Il TAC è disponibile per:

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

1. Collect Admin-Techs - Eseguire admin-tech su tutti i componenti di controllo (vSmart, vManage, vBond) prima dell'aggiornamento per evitare la perdita dei dati di diagnostica. Selezionare le opzioni Log and Tech. Core non è richiesto.

   

Attenzione: Gli admin-tech vSmart non devono essere eseguiti simultaneamente, ovvero eseguiti uno alla volta. Tutti gli altri possono essere raccolti in qualsiasi ordine

2. Aggiorna a una versione fissa - Aggiorna tutti i componenti di controllo SD-WAN (vManage, vSmart, vBond) a una versione software fissa elencata nella tabella Versioni software fissa.

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

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

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

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

Raccolta:

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

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

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

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

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

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

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

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

Passaggio 2: Aggiorna a una versione software fissa

Dopo aver raccolto gli admin-tech nella Fase 1, aggiornare tutti i componenti di controllo SD-WAN (vManage, vSmart e vBond) a una versione software fissa.

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

Selezionare la versione appropriata dalla tabella Versioni software fisso in questo documento.

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

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

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

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

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

Azioni richieste:

1. Aprire una richiesta TAC di gravità 3 con "CVE-2026-20182" e il relativo ID PSIRT nel titolo per avviare il processo di scansione.
2. Caricare TUTTI i bundle di log admin-tech raccolti nel Passo 1 (Controller, Manager e Convalide)
3. Attendere il completamento dell'analisi di TAC e comunicare i risultati

---

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

Passaggio 4: Se viene identificato un compromesso, seguire le istruzioni di TAC

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

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

Versioni software fisse

Queste versioni software contengono correzioni per le vulnerabilità identificate:

Si applica alle versioni correnti	Versione corretta	Software disponibile
20,3, 20,6, 20,9	20.9.9.1	20.9.9.1 aggiornamento delle immagini per vManage, vSmart e vBond
20.10, 20.11, 20.12.5 e precedenti nella 20.12	20.12.5.4	20.12.5.4 aggiornamento delle immagini per vManage, vSmart e vBond
20.12.6.x	20.12.6.2	20.12.6.2 aggiornamento delle immagini per

Si applica alle versioni correnti	Versione corretta	Software disponibile
		vManage, vSmart e vBond
20.12.7	20.12.7.1	20.12.7.1 aggiornamento delle immagini per vManage, vSmart e vBond
20.13, 20.14, 20.15.4.3 e precedenti del 20.15	20.15.4.4	20.15.4.4 aggiornamento delle immagini per vManage, vSmart e vBond
20.15.5.x	20.15.5.2	20.15.5.2 immagini di aggiornamento per vManage, vSmart e vBond
20.16, 20.17, 20.18.x	20.18.2.2	20.18.2.2 aggiornamento delle immagini per vManage, vSmart e vBond

Nota: per i clienti su cloud SD-WAN (precedentemente noto come cloud Delivered Cisco Catalyst SD-WAN [CDCS]), anche la versione 20.15.506 è una versione fissa. Ciò si applica in modo specifico alla distribuzione di cluster ospitati da Cisco e viene gestito separatamente dal percorso di aggiornamento standard. Tutti i clienti di questo tipo sono già stati aggiornati alla release fissa 20.15.506.

Riferimenti importanti:

- Matrice di aggiornamento
- Matrice di compatibilità dei controller

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

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

Nota:

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

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

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

Passaggio 1: Identificazione di IP di sistema vManage validi

Accedere a ciascun controller vSmart ed eseguire:

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

Output di esempio:

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                          PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                    PORT    PUBLIC I
-------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                    12346   10.1.10.1
```

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

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

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

Fase 2b: Passaggio aggiuntivo per i sistemi vManage

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

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

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

```
show control local-properties
```

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

```
show interface | tab
```

Passaggio 3: Esegui comando di verifica

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

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

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

Passaggio 4: Interpreta risultati e documento per TAC

Se non viene visualizzato alcun output:

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

Se vengono stampate le righe del log:

- Esaminare attentamente tutti gli indirizzi IP visualizzati
- Verificare che l'indirizzo IP non sia correlato all'infrastruttura vManage (IP cluster, IP sistema precedente o simile)

- Se non si riesce a identificare l'IP di origine come legittimo, ciò può indicare potenziali indicatori di compromissione
- La voce registrata nel log mostra un timestamp e un indirizzo IP di origine
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere le voci di log, i timestamp e gli IP di origine nel caso
- Il TAC determina la valutazione ufficiale

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

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

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

Accedere innanzitutto a vshell e quindi alla directory di log:

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

Eseguire quindi questo comando per eseguire una ricerca nel file vsyslog* glob:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Ripetere l'operazione per messages* file glob e vdebug* file glob.

Passaggio 2: Interpreta risultati e documento per TAC

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

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

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

- Esaminare attentamente tutti gli indirizzi IP e i tipi di peer visualizzati
- Verificare che l'indirizzo IP non sia correlato all'infrastruttura del control plane SD-WAN

- Se non si riesce a identificare l'IP di origine come legittimo, ciò può indicare potenziali indicatori di compromissione
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere l'output completo del comando con le coppie peer-type e peer-system-ip nel proprio caso
- Il TAC determina la valutazione ufficiale

Verifica 3: Verifica la presenza di challenge-ack mancanti nelle connessioni di controlli attivi

Questo controllo controlla l'output dei dettagli delle connessioni di controllo per le sessioni peer segnalate come attive (o disattivate di recente) ma senza lo scambio `Challenge-Back` previsto. Una sessione che scambia pacchetti `hello` in entrambe le direzioni mentre mostra `challenge-ack 0` nelle statistiche Tx o Rx indica che il peer non ha mai completato l'handshake di richiesta previsto — un'anomalia che richiede un'indagine. Eseguire questa operazione su tutti i componenti di controllo (Controller, Manager e Convalide).

Passaggio 1: Raccoglie l'output dei dettagli delle connessioni dei controlli

Dalla CLI del dispositivo, eseguire:

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

Salvare l'output in un file (ad esempio, `vdaemon.txt`) per l'ispezione.

Passaggio 2: Cosa cercare

Per ogni record peer (delimitato da intestazioni `REMOTE-COLOR-` / `SYSTEM-IP-`), contrassegnare il record se tutte le condizioni seguenti sono vere:

- Lo stato della sessione è UP o TEAR_DOWN
- Sia il contatore Hello statistiche Tx che il contatore Hello statistiche Rx sono diversi da zero (gli hellos scorrono in entrambe le direzioni)
- challenge-ack è 0 nel blocco Statistiche Tx o Statistiche Rx (o in entrambi)

Record corrispondente di esempio (notare le `<<<` frecce che evidenziano la `corrispondenza` mancante)

```
----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
----------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
```

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

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

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

Nell'esempio precedente, entrambi i contatori Tx e Rx `hello` sono diversi da zero (connessione attiva), ma `challenge-ack` è `0` in entrambe le direzioni.

Passaggio 3: Comando di ricerca manuale

Per visualizzare rapidamente i record candidati da un file `vdaemon.txt` salvato (o da qualsiasi file contenente l'output di `visualizzazione dei dettagli delle connessioni dei controlli`), eseguire:

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

Ogni blocco restituito rappresenta una sessione peer in cui challenge-ack è indicato come 0. Esaminare completamente ogni blocco per verificare che lo stato sia `up` o `tear_down` e che i `contatori hello` in Tx e Rx siano diversi da zero prima di considerarli un hit.

Passaggio 4: Interpreta risultati e documento per TAC

Se nessun record soddisfa tutte e tre le condizioni:

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

Se uno o più record soddisfano tutte e tre le condizioni:

- Esaminare attentamente i valori `SYSTEM-IP-`, `private-ip` e `public-ip` di ciascun record contrassegnato.

- Verificare che il peer non sia una parte nota e legittima del control plane SD-WAN (membro del cluster, sito DR, indirizzo IP precedentemente assegnato a un componente)
- Se non si riesce a identificare il peer come legittimo, ciò può indicare potenziali indicatori di compromissione
- Documentazione di tutti i risultati e apertura immediata di una richiesta TAC
- Includere i record peer corrispondenti completi e l'output del comando di origine nel caso specifico
- Il TAC determina la valutazione ufficiale

Domande frequenti

Q: Qual è il primo passo per affrontare questo advisory della sicurezza?

A: Raccogliere i file admin-tech da tutti i componenti di controllo, quindi aggiornare tutti i componenti di controllo a una versione software fissa. Dopo l'aggiornamento, aprire una richiesta TAC e caricare gli admin-tech in modo che TAC possa analizzare l'ambiente per rilevare eventuali indicatori di compromesso.

D. A quale versione devo effettuare l'aggiornamento?

R. Eseguire l'aggiornamento alla versione fissa più vicina al più presto.

Q: È necessario raccogliere gli admin-tech da tutti i componenti di controllo?

A: Sì, TAC richiede file admin-tech da tutti i controller (vSmart, raccolti uno alla volta), da tutti i manager (vManage) e da tutti i validatori (vBond) per valutare correttamente l'ambiente.

Q: In che modo TAC determina se il sistema è stato compromesso?

A: TAC analizza i file admin-tech utilizzando strumenti specializzati per valutare l'ambiente del cliente alla ricerca di indicatori di compromesso.

Q: Esiste un modo per eseguire la scansione automatica utilizzando gli strumenti TAC?

A: Per ripetere l'analisi degli admin-tech dai componenti di controllo, i clienti possono anche usare lo strumento self-service "Check Bug Applicability" incorporato nella pagina Bug Search Tool per l'ID bug Cisco CSCwt50498.

Q: Cosa succede se vengono individuati indicatori di compromesso?

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

Q: Come è possibile sapere quale versione software fissa utilizzare?

A: Fare riferimento alla tabella Versioni software fisso in questo documento. TAC conferma la versione appropriata per l'ambiente specifico.

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

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

Q: Durante il monitoraggio e l'aggiornamento è previsto il downtime?

A: L'impatto dipende dall'architettura di distribuzione e dal percorso di correzione. TAC fornisce indicazioni per ridurre al minimo l'impatto dei servizi durante il processo.

Q: È necessario aggiornare tutti i controller se non vengono rilevati indicatori di compromissione?

A: Sì, tutti i componenti di controllo SD-WAN (vManage, vSmart e vBond) devono essere aggiornati a una versione software fissa. Non è sufficiente aggiornare solo un sottoinsieme di controller.

Q: Ho un overlay SD-WAN ospitato dal cloud. Quali sono le opzioni per l'aggiornamento?

A: Per le sovrapposizioni ospitate nel cloud, i clienti hanno due opzioni:

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

Q: È necessario aggiornare anche i router perimetrali?

A: No, i dispositivi Cisco IOS XE non sono interessati da questo avviso.

D: Siamo un Cisco hosted overlay. È necessario correggere gli ACL o eseguire azioni sul provider di servizi condivisi?

A: Tutti i clienti ospitati da Cisco sono invitati a rivedere le proprie regole consentite per il traffico in entrata visualizzate sul provider di servizi condivisi e ad accertarsi che siano consentiti solo i prefissi necessari dal lato dell'utente. Queste regole sono valide solo per l'accesso alla gestione e non si applicano ai router perimetrali. Esaminarli in SSP > Sovrapponi dettagli > Consenti regole in entrata. La porta 22 e 830 è sempre stata bloccata per impostazione predefinita nel giorno 0 del provisioning da Cisco dall'esterno ai controller ospitati nel cloud.

Q: Siamo su SD-WAN Cloud (noto in precedenza come Cloud Delivered Cisco Catalyst SD-WAN [CDCS]). A quale versione verrà eseguito l'aggiornamento?

A: In base alla versione corrente, i cluster cloud SD-WAN sono attualmente in programma per essere aggiornati O già aggiornati alle versioni fisse. Di seguito sono riportate le versioni fisse di SD-WAN Cloud (in precedenza CDCS):

1. Cluster Early Adopter = 20.18.2.2 (in realtà è la stessa versione standard)

2. Cluster release consigliati = 20.15.506 (versione specifica CDCS con correzioni PSIRT)

I clienti del cloud SD-WAN non devono intraprendere alcuna azione efficace per risolvere questo problema.

Q: Siamo su un tenant condiviso. A quale versione verrà eseguito l'aggiornamento?

A: In base alla versione corrente, il tenant condiviso è attualmente pianificato per l'aggiornamento O è già stato aggiornato alle versioni fisse. Ecco le versioni fisse del tenant condiviso:

1. Cluster release consigliati = 20.15.5.2

Q: Cisco TAC fornisce servizi di analisi forense o di indagine per queste vulnerabilità?

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

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

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

Q: Nel sistema vengono visualizzati i log di un utente "root". Questo è preoccupante?

A: Controllare che cosa altro sta succedendo nel sistema in quel momento. Questi registri sono assolutamente prevedibili. Ad esempio, i log delle modifiche all'accesso di sistema di un utente "root" vengono visualizzati quando vengono generati gli admin-tech. I registri possono anche essere visualizzati da un utente "root" durante un riavvio.

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

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

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

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

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).