修正Catalyst SD-WAN安全建議 — 2026年5月

目錄

簡介

本文檔介紹根據2026年5月14日的PSIRT公告識別和修復SD-WAN中關鍵安全漏洞的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst SD-WAN架構和控制元件(vManage、vSmart、vBond)
- Cisco Catalyst SD-WAN升級程式
- Cisco TAC案件管理和管理技術收集程式

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

有關詳細的背景資訊和最新更新，請參閱官方PSIRT諮詢頁面。

可從以下連結獲得以下建議：

- Cisco Catalyst SD-WAN控制器驗證旁路漏洞
- Cisco Catalyst SD-WAN漏洞

以下PSIRT建議可以解決這些缺陷：

- 思科錯誤ID CSCwt50498
- 思科錯誤ID CSCwt38739
- 思科錯誤ID CSCwt38767
- 思科錯誤ID CSCwt55544

補救工作流概述

附註：所有SD-WAN控制器和管理器都易受攻擊，需要立即升級所有控制元件。但是，並非所有控制器都顯示有危害跡象。

所需操作：收集管理技術，升級至固定版本，然後開啟思科TAC案例，以便TAC可以掃描您的管理技術，尋找危害跡象。

TAC可用於：

- 掃描您提供的管理技術以發現危害跡象
- 如果在升級過程中遇到問題，則提供升級支援
- 如果識別出危害跡象，則引導您進行其他補救

1. 在升級之前，收集管理技術 — 對所有控制元件(vSmart、vManage、vBond)運行管理技術，以確保診斷資料不會丟失。選擇「日志」和「技術」選項。 不需要核心。

   注意：vSmart管理技術不能同時運行 — 一次運行一個。其他所有項都可以按任意順序收集

   ---

2. 升級到固定版本 — 將所有SD-WAN控制元件(vManage、vSmart、vBond)升級到「固定軟體版本」(Fixed Software Versions)表中列出的固定軟體版本。

   附註：升級前不要等待TAC掃描結果。升級到固定版本是最高優先順序並會關閉漏洞

。 步驟3中的TAC掃描可確定升級後是否需要執行任何進一步操作。

3. 開啟TAC案件並上傳管理技術以掃描危害指標 — 開啟思科TAC案件並上傳步驟1中收集的所有管理技術日誌套件。TAC掃描管理技術以尋找危害指標。
4. 如果識別出危害，請遵循TAC指南 — 如果TAC識別出您環境中的危害表現，請完成TAC提供的所有補救指南。如果沒有發現危害跡象，則無需在升級後執行進一步的操作。

步驟 1:從所有控制元件收集管理技術檔案

必需：在升級前從所有控制元件收集管理技術檔案，以確保不會丟失任何診斷資料。TAC在第3步使用這些檔案來掃描您的環境，尋找危害跡象。

集合：

附註：對於admin-tech generation，請選擇Log and Tech options。 不需要核心。

1. 在所有控制器(vSmarts)上運行管理技術 — 不要同時運行這些控制器；一次收集一個
2. 在所有管理器上運行管理技術(vManagers)
3. 在所有驗證器上運行管理技術(vBonds)

附註：vSmart管理技術不能同時運行 — 一次收集一個。可以按任意順序收集管理員和驗證程式的管理技術。

在SD-WAN環境中收集管理技術並上傳到TAC案例

附註：TAC會分析這些檔案以評估您的環境是否受到危害，並指導適當的補救路徑。

替代方案：手動驗證（僅當無法收集管理技術時）

對於無法共用管理技術檔案的使用者，可使用手動驗證步驟。這些步驟提供必須記錄並與TAC共用的初始指標。

如需詳細程序，請參閱本文結尾的「手動驗證步驟」一節。記錄所有調查結果，並在您的支援案例中將其提供給TAC。

步驟 2:升級至固定軟體版本

在步驟1中收集管理技術後，將所有SD-WAN控制元件（vManage、vSmart和vBond）升級到固定軟體版本。

⚠ 重要：升級前不要等待TAC掃描結果。升級到固定版本是最高優先順序並會關閉漏洞。步驟3中的TAC掃描可確定升級後是否需要任何進一步的操作。

從本文檔的固定軟體版本表中選擇適當的版本。

警告：升級必須保持在您目前的主要版本中。如果沒有明確的TAC指導，請勿升級到更高的主要版本。

使用vManage GUI或CLI升級SD-WAN控制器

附註：如果您在升級期間遇到任何問題，請開啟TAC案例以取得升級支援。

步驟 3:開啟TAC案件並上傳管理技術檔案以進行掃描

在第2步升級後，開啟Cisco TAC支援案件，並上傳第1步中收集的管理技術檔案。TAC掃描管理技術以尋找危害指標。

所需操作：

1. 使用「CVE-2026-20182」和標題中的相關PSIRT ID開啟嚴重性3 TAC案例，以啟動掃描流程。
2. 上傳步驟1中收集的所有管理技術日誌捆綁包（控制器、管理器和驗證器）
3. 等待TAC完成掃描並傳送結果

附註：TAC分析管理技術檔案並傳達掃描結果。如果沒有發現危害跡象，則無需在升級後執行進一步的操作。

步驟 4:如果識別出危害 — 請遵循TAC指南

如果TAC識別出您環境中的危害表現，TAC會與您聯絡，提供具體的補救指南。完成TAC提供的所有說明。

如果未識別出任何危害跡象，則步驟2中完成的升級就足夠了，無需進一步的補救。

固定軟體版本

這些軟體版本包含已識別漏洞的修正程式：

應用於當前版本	已修正的版本	可用軟體
20.3、20.6、20.9	20.9.9.1	20.9.9.1適用於vManage、vSmart和vBond的升級映像
20.10、20.11、20.12.5及20.12中的更早版本	20.12.5.4	20.12.5.4 vManage、vSmart和vBond升級映像
20.12.6.x	20.12.6.2	20.12.6.2適用於vManage、vSmart和vBond的升級映像
20.12.7	20.12.7.1	20.12.7.1適用於vManage、vSmart和vBond的升級映像
20.13、20.14、20.15.4.3及20.15中的更早版本	20.15.4.4	20.15.4.4針對vManage、vSmart和vBond的升級映像
20.15.5.x	20.15.5.2	適用於vManage、vSmart和vBond的20.15.5.2升級映像
20.16、20.17、20.18.x	20.18.2.2	適用於vManage、vSmart和vBond的20.18.2.2升級映像

註：對於SD-WAN雲（以前稱為雲交付Cisco Catalyst SD-WAN [CDCS]）上的客戶，20.15.506也是固定版本。這特別適用於思科託管的群集部署，並且與標準升級路徑分開處理。所有此類客戶都已升級到固定版本20.15.506。

重要參考資料：

- 升級表
- 控制器相容性矩陣

附錄:手動驗證步驟（僅當無法進行管理技術收集時）

附註：Admin-tech集合是首選和推薦的方法。僅當完全無法收集和共用管理技術檔案時才使用手動驗證。如果無法收集管理技術檔案，請使用以下手動步驟收集TAC的初步指標。

附註：

- 這些步驟僅提供初步資料
- 強烈建議管理員技術收集以進行準確評估
- 記錄您的調查結果，並在您的支援案例中與TAC分享這些調查結果
- TAC作出正式評估決定

要求:必須在所有控制元件上執行這些步驟。

驗證 1:在身份驗證日誌中檢查未經授權的SSH登入

步驟 1:確定有效的vManage系統IP

存取每個vSmart控制器並執行：

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

輸出示例：

```
                                                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
```

步驟 2:生成正規表示式字串（僅限vBond和vSmart）

將第1步中的所有系統IP合併為OR regex模式：

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

第2b步：vManage系統的附加步驟

如果在vManage本身上運行這些命令，則將localhost IP(127.0.0.1)、本地系統IP、所有群集IP和VPN 0傳輸介面IP附加到regex:

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

要查詢本地vManage系統IP，請使用：

```
show control local-properties
```

要查詢VPN 0傳輸介面IP和集群IP，請使用：

```
show interface | tab
```

步驟 3:執行驗證命令

運行以下命令，用第2步中的正規表示式字串替換REGEX:

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

附註：此命令過濾身份驗證日誌，以便只顯示來自意外源的vmanage-admin登入。合法登入必須僅源自vManage相關IP。

步驟 4:解釋TAC的結果和檔案

如果未顯示輸出：

- 在此裝置上未檢測到危害跡象
- 記錄您的TAC案例的此結果
- 繼續評估其餘控制器

如果列印日誌行：

- 仔細檢查所示的每個IP地址
- 驗證IP與vManage基礎設施（集群IP、舊系統IP或類似的）無關
- 如果不能將源IP標識為合法，則這可能表示存在潛在危害跡象
- 日誌條目顯示時間戳和源IP地址
- 記錄所有調查結果並立即建立TAC案例
- 在案例中包括日誌條目、時間戳和源IP

- TAC執行正式評估確定

驗證 2:檢查控制器系統日誌中是否有未授權的對等連線

此命令從控制器系統日誌檔案中提取所有對等型別對和對等系統IP對，並將其輸出為供您檢視的清單。它不會自動標籤可疑條目 — 您必須檢查輸出並確定每個對等系統IP是否是SD-WAN基礎架構的已知合法部分。在所有控制元件（控制器、管理器和驗證器）上運行此命令。

步驟 1:在每個控制元件上運行命令：

首先，訪問vshell並導航到日誌目錄：

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

然後運行以下命令搜尋vsyslog*檔案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
```

對messages* file glob和vdebug*file glob重複此操作。

步驟 2:解釋TAC的結果和檔案

如果輸出僅顯示已知的vManage/vSmart/vBond系統IP:

- 未從此檢查中檢測到任何危害跡象
- 記錄您的TAC案例的此結果
- 繼續評估其餘控制元件

如果輸出包含無法識別的對等系統IP:

- 仔細檢查所示的每個IP地址和對等型別
- 驗證IP是否與已知的SD-WAN控制平面基礎設施無關
- 如果不能將源IP標識為合法，則這可能表示存在潛在危害跡象
- 記錄所有調查結果並立即建立TAC案例
- 在您的案例中包括peer-type和peer-system-ip對的完整命令輸出
- TAC執行正式評估確定

驗證 3:檢查活動控制連線上缺少質詢確認

此檢查會檢查報告為活動（或最近關閉）但缺少預期的challenge-ack交換的對等會話的control

connections detail輸出。在Tx或Rx統計資訊中顯示challenge-ack 0時，雙向交換hello資料包的會話表示對等裝置從未完成預期的challenge握手 — 此異常值得進行調查。在所有控制元件（控制器、管理器和驗證器）上運行此命令。

步驟 1:收集控制連線詳細資訊輸出

從裝置CLI運行：

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

將輸出儲存到檔案(例如vdaemon.txt)以供檢查。

步驟 2:尋找什麼

對於每個對等記錄(以REMOTE-COLOR- / SYSTEM-IP-標頭分隔)，如果以下所有條件都為真，請標籤該記錄：

- 會話狀態為UP或TEAR_DOWN
- Tx Statistics hello計數器和Rx Statistics hello計數器均不為零（hello在雙向流動）
- challenge-ack is 0 in the Tx Statistics or Rx Statistics block（或both）

匹配記錄示例(請註意<<<箭頭，突出顯示缺少的challenge-ack)

```
------------------------------------------------------------------------------------------------
 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)
...
```

在上方範例中，Tx和Rx hello計數器都是非零（作用中連線），但兩個方向的challenge-ack均為0。

步驟 3:手動搜尋命令

要從儲存的vdaemon.txt(或包含show control connections detail輸出的任何檔案)中快速呈現候選記錄，請運行：

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

返回的每個塊表示一個對等會話，其中challenge-ack報告為0。請完整檢視每個塊，以確認狀態為up或tear_down，並且Tx和Rx中的hello計數器均非零，然後再將其視為命中。

步驟 4:解釋TAC的結果和檔案

如果沒有滿足所有三個條件的記錄：

- 未從此檢查中檢測到任何危害跡象
- 記錄您的TAC案例的此結果
- 繼續評估其餘控制元件

如果一個或多個記錄滿足所有三個條件：

- 仔細檢查每個標籤的記錄的SYSTEM-IP-、private-ip和public-ip值
- 驗證對等體不是SD-WAN控制平面中已知的合法部分（集群成員、DR站點、以前分配給元件的IP地址）
- 如果您無法識別對等體是合法的，這可能表示存在潛在危害跡象
- 記錄所有調查結果並立即建立TAC案例
- 在您的案例中包括完全匹配的對等記錄和源命令輸出
- TAC執行正式評估確定

常見問題

Q:解決此安全建議的第一步是什麼？

A:從所有控制元件收集管理技術檔案，然後將所有控制元件升級到固定的軟體版本。升級後，開啟TAC案件並上傳管理技術，以便TAC可以掃描您的環境是否有危害跡象。

問：我需要升級至哪個版本？

A.請儘早升級到最近的固定版本。

Q:我是否需要從所有控制元件收集管理技術？

A:是，TAC要求所有控制器（vSmart，一次收集一個）、所有管理員(vManage)和所有驗證器(vBond)提供管理技術檔案，以正確評估您的環境。

Q:TAC如何確定我的系統是否已被破壞？

A:TAC使用專用工具分析管理技術檔案，以評估您的環境是否存在危害跡象。

Q:是否有辦法使用TAC工具執行我自己的自動掃描？

A:客戶也可使用自助「檢查錯誤適用性」工具(內建在Bug Search Tool頁面上，適用於思科錯誤ID CSCwt50498)，從控制元件重新掃描管理技術。

Q:如果識別出危害表現會怎樣？

A:TAC會與您聯絡，討論針對您的環境的後續步驟和指南。思科不會代表您執行補救 — TAC提供您繼續操作所需的指導。

Q:如何知道使用哪個固定軟體版本？

A:請參閱本檔案的固定軟體版本表。TAC會確認適用於您特定環境的適當版本。

Q:在TAC分析我的管理技術之前，我能否開始升級？

A:會。收集管理技術，升級至固定版本，然後開啟TAC案例，使TAC可以掃描管理技術以尋找危害跡象。

Q:補救期間是否預計停機？

A:影響取決於您的部署架構和補救路徑。TAC提供在此過程中將服務影響降至最低的指導。

Q:如果找不到危害跡象，是否需要升級所有控制器？

A:是的，所有SD-WAN控制元件（vManage、vSmart和vBond）都必須升級到固定軟體版本。僅升級控制器的子集是不夠的。

Q:我有雲託管SD-WAN覆蓋。我的升級選項是什麼？

A:對於雲託管的重疊，客戶有兩種選擇：

1. 通過導航到SSP >重疊詳細資訊>更改視窗，檢查您的環境是否計畫進行自動升級。
2. 如果您不想等待計畫的升級，則有兩個選項：
    - 使用本文檔中提供的升級指南自行升級。
    - 開啟備用TAC案例，用於您的首選維護視窗。如果您在升級過程中遇到困難，TAC可為您提供幫助。

Q:我們是否需要升級邊緣路由器？

A:否，Cisco IOS XE裝置不受此建議的影響。

問：我們是思科託管覆蓋層。是否需要修復任何ACL或對SSP執行操作？

A:建議所有思科託管客戶檢視其自身在SSP上看到的允許入站規則，並確保僅允許來自您一側的必要字首。這些規則僅適用於管理訪問，並且不適用於邊緣路由器。請在SSP >重疊詳細資訊>允許入站規則中檢視這些規則。請注意，思科在第0天從外部調配到雲託管控制器時，預設情況下始終阻止埠22、830。

Q:我們處於SD-WAN雲端（以前稱為雲交付的Cisco Catalyst SD-WAN [CDCS]）。 我們將升級到哪個版本？

A:根據當前版本，SD-WAN雲群集目前按計畫進行升級或已經升級到固定版本。以下是SD-WAN Cloud（前身為CDCS）固定版本：

1.早期採用者集群= 20.18.2.2（這實際上與標準版本相同）

2.建議版本群集= 20.15.506(帶PSIRT修復的CDCS特定版本)

SD-WAN雲客戶無需採取任何有效措施來解決此PSIRT。

Q:我們在共用租戶上。我們將升級到哪個版本？

A:根據當前版本，共用租戶當前按計畫進行升級，或者已升級到固定版本。以下是共用租戶固定版本：

1.建議版本群集= 20.15.5.2

Q:Cisco TAC是否為這些漏洞提供取證分析或調查服務？

A:Cisco TAC可通過掃描與這些漏洞相關的危害表現(IoC)來協助客戶。但是，TAC不會執行深入的法證分析或事件調查。對於全面的調查分析工作或詳細的安全調查，我們建議客戶與其首選的第三方事件響應(IR)公司接洽。

Q:針對我的SD-WAN重疊降低漏洞的一般最佳實踐或方法是什麼？

A:請參閱Cisco Catalyst SD-WAN加固指南，瞭解減少SD-WAN重疊中的漏洞的最佳實踐和建議。

Q:我們將看到系統上「root」使用者的日誌。 這有關係嗎？

A:檢查系統當時還發生了什麼情況。 這些日誌完全可以預期。 例如，生成admin-techs時，會看到來自「root」使用者的系統登入更改日誌。 在重新引導期間，也可以從「root」使用者處看到日誌。

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。