修正Catalyst SD-WAN安全建議 — 2026年2月

目錄

簡介

本文檔介紹根據2026年2月25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漏洞
- Cisco Catalyst SD-WAN控制器驗證旁路漏洞

以下PSIRT建議可以解決這些缺陷：

- 思科錯誤ID CSCws52722
- 思科錯誤ID CSCws33583
- 思科錯誤ID CSCws33584
- 思科錯誤ID CSCws33585
- 思科錯誤ID CSCws33586
- 思科錯誤ID CSCws33587
- 思科錯誤ID CSCws93470

補救工作流概述

附註：所有SD-WAN部署都易受攻擊，需要立即採取行動。但是，並非所有系統都顯示存在危害的跡象。

所需操作：建立思科TAC案例，解決此安全建議問題。

TAC可用於：

- 評估您的環境是否有危害表現
- 根據評估指導您完成適當的補救路徑
- 如果識別出危害跡象，則與PSIRT團隊合作
- 如果未檢測到危害跡象，則提供升級指導和支援

1. 收集管理技術 — 對所有控制元件(vSmart、vManage、vBond)運行管理技術。vSmart管理技術不能同時運行 — 一次運行一個。其他所有資訊都可以按任意順序收集。選擇「Log and Tech（日誌和技術選項）」。 不需要核心。
2. 開啟TAC案例 — 聯絡思科TAC並提供所有控制元件管理技術日誌捆綁包
3. TAC評估- TAC評估您的環境是否有危害表現
4. 執行補救 — 完成TAC提供的特定流程

步驟 1:從所有控制元件收集管理技術檔案

必需：在開啟TAC案例之前，從所有控制元件收集管理技術檔案。對於TAC評估您的環境，這是至關重要的。

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:開啟TAC案件並上傳管理技術檔案

從步驟1收集所有管理技術檔案後，開啟Cisco TAC支援案例。

所需操作：

1. 開啟具有適用於您業務影響的嚴重性層級的TAC案例
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. 參考PSIRT諮詢
4. 等待TAC評估和指南

⚠

注意：TAC確定您的系統的狀態並推薦適當的後續步驟。

如果沒有得到TAC指導，請勿嘗試進一步步驟

步驟 3:TAC評估

TAC會分析上傳的管理員技術檔案，並確定您的系統狀態。

在此期間：

- 等待TAC進行正式評估，然後再採取任何措施
- TAC會聯絡您提供其調查結果以及後續步驟

步驟 4:執行補救（TAC指導）

TAC會根據您的評估指導您完成適當的補救流程。完成TAC提供的所有說明。

路徑A:未找到危害表現 — 升級

如果TAC確認沒有受到危害的跡象，請升級至固定軟體版本。從本文檔的固定軟體版本表中選擇適當的版本，並參考本節中連結的升級指南。

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

路徑B:確定的危害表現 — PSIRT指導的

如果TAC確認存在危害表現，他們可委託PSIRT團隊制定針對您環境的自定義補救策略。完成TAC和PSIRT提供的所有指南。

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	20.9.8.2 *	20.9.8.2適用於vManage、vSmart和vBond的升級映像

應用於當前版本	已修正的版本	可用軟體
20.10、20.11、20.12.5及20.12中的更早版本	20.12.5.3	適用於vManage、vSmart和vBond的20.12.5.3升級映像
20.12.6	20.12.6.1	20.12.6.1適用於vManage、vSmart和vBond的升級映像
20.13、20.14、20.15.x	20.15.4.2	20.15.4.2適用於vManage、vSmart和vBond的升級映像
20.16、20.17、20.18.x	20.18.2.1	20.18.2.1適用於vManage、vSmart和vBond的升級映像

附註：對於CDCS(思科託管集群)上的客戶,20.15.405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。

*如果您使用的是20.9版或更低版本：您版本(20.9.8.2)的固定軟體於2027年2月27日提供。思科建議保留在當前主要版本中並等待20.9.8.2版本，而不是升級到更高的主要版本(20.12、20.15、20.18)。 如果您目前的版本低於20.9，請等待20.9.8.2升級。繼續與TAC合作，並於2027年2月複查，瞭解可用的軟體連結。

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
```

然後執行以下命令：

```
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
```

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

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，並開啟TAC案例以上傳檔案。TAC會評估您的環境並提供後續步驟的指導。

我應該升級至哪個版本？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:如果識別出危害表現會怎樣？

A:TAC會與PSIRT團隊聯絡，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:否，等待TAC完成評估並提供指導，然後嘗試任何補救操作。

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:即將發佈的20.15.5版本和其他即將發佈的版本是否包括PSIRT修復？

A:是，20.15.5版和其他即將發佈的版本中包括修復。但是，必須立即優先執行用於緩解本文檔中概述的漏洞的升級。（不要等待！）

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。如果您在升級時遇到困難，TAC將為您提供幫助。

Q:我們是否需要升級邊緣路由器？

A: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。

問：我們使用CDCS/共用租戶。我們將升級到哪個版本？

A:根據當前版本，共用租戶或CDCS群集當前按計畫進行升級或已經升級到固定版本。以下是共用租戶和CDCS固定版本：

1. Early Adopter clusters => 20.18.2.1（這實際上與標準版本相同）

2.建議版本集群=> 20.15.405（CDCS特定版本帶PSIRT修復）

CDCS客戶無需採取有效措施來解決此PSIRT問題。

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。

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）。