修正Catalyst SD-WAN安全建議 — 2026年6月

目錄

簡介

本文檔介紹根據2026年6月4日發佈的PSIRT公告識別和解決SD-WAN中的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 Manager驗證許可權提升漏洞

以下PSIRT建議可以解決這些缺陷：

- 思科錯誤ID CSCwu18563

補救工作流概述

此建議描述了SD-WAN Manager中需要使用netadmin許可權進行攻擊的許可權提升漏洞。

根據建議，未經身份驗證的遠端攻擊者獲取這些許可權的已知路徑是利用CVE-2026-20182(cisco-sa-sdwan-rpa2-v69WY2SW)或CVE-2026-20127(cisco-sa-sdwan-rpa-EHchtZk)。

如果您的控制元件已升級到這兩個公告的固定版本，且思科在您為以前事件提供的管理技術檔案中未發現任何潛在危害表現(IoC)，則根據已檢查的檔案，這些特定裝置上針對此新漏洞的已知未經驗證攻擊路徑將被緩解。

這並不能消除攻擊者持有有效netadmin憑據時的風險。思科尚未發佈針對此漏洞的軟體修補程式，也沒有可用的解決方法；進一步指導將隨後提供。

所需操作：開啟思科TAC案例解決此安全建議。

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
- 就確定危害表現之後需要採取的後續步驟提供指導

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 — 對您環境中的危害表現進行初步評估，然後TAC對您環境中的危害表現進行初步評估。
4. 執行補救 — 如果需要，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：在任何升級或配置更改之前，從所有控制元件收集管理技術文件，以便保留診斷資料和任何

潛在危害表現(IoC)。TAC在第3步使用這些檔案來分析您的環境。

集合：對於管理技術生成，請選擇「日誌」和「技術」選項。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)

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，以瞭解與此諮詢相關的危害表現。本諮詢的分析側重於特定日誌條目，該條目不能區分合法和惡意使用；需要由TAC手動稽核。

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客戶，可使用手動驗證步驟。此步驟提供必須記錄並與TAC共用的初步指標。

如需詳細程式，請參閱本檔案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

在步驟1中收集管理技術後，開啟Cisco TAC支援案例，並上傳收集的管理技術檔案。TAC會分析管理技術人員，以瞭解與此建議相關的危害指標。

所需操作：

1. 使用「CVE-2026-20245」和標題中的建議ID `cisco-sa-sdwan-privesc-4uxFrdzx`開啟嚴重性3 TAC案例，以啟動分析。
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完成分析並傳送結果。

附註：思科尚未發佈針對此漏洞的軟體修復程式，並且沒有可用的解決方法。步驟3中的TAC分析有助於確定您提供的管理技術檔案中是否存在任何危害表現。在工程部門提供進一步指導後，將遵循該指南。

步驟 3:TAC評估

TAC會初步分析您在第2步上傳的管理技術檔案，並評估這些檔案是否有與此建議相關的危害表現。

對於此建議，分析重點放在/var/log/scripts.log中每個Manager(vManage)上的特定日誌條目。 由於基礎命令是合法的，並且日誌不能區分合法和惡意使用，因此任何匹配的條目需要由TAC根據客戶的正常運行狀態進行手動稽核，然後才被視為已確認的指示器。

TAC分析的可能結果：

- 未標識匹配的日誌條目 — 根據稽核的管理技術檔案，未發現與此諮詢相關的指示符。目前無需針對此建議採取任何進一步行動。結果僅限於收到的管理技術檔案，可能受到每台裝置上的日誌保留期的限制。
- 已識別匹配日誌條目 — TAC將通過其他稽核步驟與客戶接洽。由於思科尚未為此建議發佈軟體修補程式，因此僅升級並不能解決此漏洞。TAC對已確認危害方案的指導記錄在步驟4中引用的相關TechZone文章中。

附註：根據建議，攻擊此漏洞需要具有netadmin許可權，未經身份驗證的攻擊者只能通過有效憑據或利用CVE-2026-20182或CVE-2026-20127來獲取此許可權。如果針對這兩個建議將您的控制元件升級到固定版本，並且未針對之前的事件識別出危害跡象，則基於所檢視的檔案，針對此新漏洞的已知未經身份驗證的攻擊路徑將在這些特定裝置上得到緩解。

步驟 4:如果識別出危害表現 — 請遵循TAC指南

如果TAC識別到您環境中與此建議相關的危害表現，TAC會根據特定指南與您聯絡。完成TAC提供的所有說明。

如果對此諮詢未確定危害表現，則根據稽核的管理技術檔案，此時無需針對此諮詢採取進一步措施。

重要：思科尚未發佈針對此顧問的軟體修復程式，且沒有可用的變通辦法。由於攻擊此漏洞需要通過CVE-2026-20182或CVE-2026-20127獲取的netadmin許可權，因此客戶應確保完成這些先前建議的補救。請參閱已建立的修正流程的相應文檔：

注意事項

在成功補救結束時，根據每個客戶的具體安全保證要求，客戶可能希望評估以下安全措施活動並採取行動。無論選擇哪種補救選項，這些活動都會適用。它們由客戶管理；思科不會代表客戶指示或執行這些操作。

- 稽核所有本地使用者帳戶
- 憑據輪替
- 裝置配置中存在的所有機密的輪替，例如（非詳盡清單）：
    - 本地使用者帳戶的憑據

    - SNMP社群字串
    - TACACS金鑰
    - VPN預先共用金鑰和憑證
    - 受信任的SSH金鑰
- 配置模板審查

邊緣裝置 — 可疑的危害

思科不建議使用特定修正路徑；補救選項的選擇取決於客戶。作為評估其環境的客戶的資訊說明：在客戶懷疑邊緣裝置受到危害時，受影響邊緣裝置的出廠重置和重新註冊是客戶在選擇邊緣裝置時可能希望考慮的一項客戶管理的操作。是否採用這種方法以及選擇哪個選項取決於客戶。

執行安全出廠重置的正確命令是：

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

固定軟體版本

> ⚠ 重要：在本文檔發佈時，Cisco尚未發佈解決CVE-2026-20245的軟體修復。根據建議，Cisco計畫在未來版本中解決Cisco Catalyst SD-WAN Manager中的此漏洞。沒有因應措施。此部分將在固定軟體可用時更新。

由於利用此漏洞需要未經身份驗證的攻擊者只能通過CVE-2026-20182或CVE-2026-20127獲取的netadmin許可權，因此鼓勵客戶確保其控制元件運行固定版本，以供以前諮詢使用。2026年5月14日SD-WAN安全建議和相應的TechZone文檔中記錄了針對這些建議的固定版本：

- Cisco Catalyst SD-WAN控制器身份驗證旁路漏洞（2026年5月14日）
- （固定軟體版本表）

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集合是首選方法。如果無法收集管理技術檔案並與TAC共用，請僅使用下面的手動驗證步驟。該手動步驟的結果是初步的；記錄調查結果並與TAC共用，TAC將

執行正式評估。

附註：對於此建議，手動驗證包括單一目標日誌檢查。搜尋到的日誌條目由合法命令生成，僅日誌不能區分合法和惡意使用。任何匹配的條目都必須根據客戶的正常運行狀態進行檢查，然後才能作為潛在指示符。如果配對專案無法與正常操作協調，請將發現結果記錄下來並與TAC共用。

驗證：在每個管理器(vManage)上檢查scripts.log，以查詢租戶清單上傳條目

根據PSIRT建議，鼓勵客戶審計位於/var/log/的scripts.log檔案，以查詢與以下示例類似的條目：

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

步驟 1:訪問每個Manager(vManage)上的vshell並搜尋日誌檔案

在vManage CLI中，放入vshell並運行：

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

對部署中的每個vManage（包括所有群整合員和任何DR配對的vManage）重複該檢查。

步驟 2:解釋TAC的結果和檔案

如果未返回匹配條目：

- 在此裝置上的日誌檔案中沒有觀察到與此建議相關的危害表現。
- 為TAC案例記錄此結果（包括裝置主機名以及搜尋的日誌檔案的日期/範圍）。
- 繼續檢查其餘的Managers。

如果返回匹配條目：

- 必須根據客戶的正常運行狀態檢查每個匹配條目。基礎命令（租戶清單上傳）是合法的，可能會在日常操作期間出現。
- 對於每個匹配條目，請捕獲時間戳、完整日誌行以及-cli後引用的文件路徑。
- 如果匹配條目無法與已知的合法操作協調，則這可能是一種危害表現。將調查結果記錄下來並交給TAC以供稽核。
- 記錄所有調查結果並建立TAC案例。包括匹配日誌條目和source命令輸出。
- TAC執行正式評估。如果評估發現危害表現，請遵循相關TechZone文檔中所述的流程：和補救指南。

常見問題

Q:解決此安全建議的第一步是什麼？

A:在任何升級或配置更改之前，從所有控制元件(vSmart、vManage、vBond)收集管理技術檔案，以儲存診斷資料和任何潛在危害指標。然後開啟思科TAC案件並上傳管理技術，以便TAC可以分析這些案例。

Q:思科是否已針對此漏洞發佈了軟體修復程式？

A:在本文檔發佈時未提供。根據建議，思科計畫在未來版本中解決Cisco Catalyst SD-WAN Manager中的此漏洞。沒有因應措施。當固定版本可用時，將更新此文檔。

Q:如果沒有修復，為什麼思科現在建議採取任何措施？

A:利用此漏洞需要netadmin許可權。根據建議，未經身份驗證的攻擊者只能通過有效憑據或通過利用CVE-2026-20182或CVE-2026-20127獲取這些許可權。確保將以前的建議中的控制元件升級到固定版本，從而通過已知未經身份驗證的路徑獲取利用此漏洞所需的許可權。第3步中的管理技術分析有助於確定所檢視的檔案中是否存在任何危害表現。

Q:我是否需要從所有控制元件收集管理技術？

A:會。TAC需要來自所有控制器（vSmart，一次收集一個）、所有管理器(vManage)和所有驗證器(vBond)的管理技術檔案才能執行分析。

Q:TAC如何確定我的系統是否有與此建議相關的危害表現？

A:TAC會檢視管理技術檔案，並在每個Manager上查詢`/var/log/scripts.log`中的PSIRT建議中所述的特定日誌條目。基礎命令是合法的；任何匹配的條目必須根據您的正常操作狀態進行檢查，然後才能作為潛在指示符。TAC執行稽核。

Q:如果識別出危害表現會怎樣？

A:TAC會根據特定指南聯絡您。由於此建議目前沒有可用的軟體修正程式，因此僅憑升級無法解決已確認的危害。TAC的指南遵循2026年5月和2026年2月諮詢相關TechZone文章中記錄的流程。

Q:邊緣路由器(Cisco IOS XE)是否受此建議的影響？

A:此建議會影響Cisco Catalyst SD-WAN Manager。根據建議，思科觀察到利用此漏洞導致配置更改推至邊緣裝置的有限案例；建議客戶驗證其邊緣裝置的配置。

Q:哪些部署型別受到影響？

A:根據建議，無論裝置配置如何，此漏洞都會影響所有Cisco Catalyst SD-WAN Manager部署型別，包括內部部署、Cisco SD-WAN Cloud-Pro、Cisco SD-WAN Cloud(Cisco Managed)和Cisco SD-WAN for Government(FedRAMP)。

Q:我已經為2026年5月和2026年2月的公告進行了升級，沒有為這些事件確定任何折衷指標。我是否暴露在這種新的漏洞之下？

A:如果您的控制元件正在為CVE-2026-20182和CVE-2026-20127運行固定版本，並且所檢視的管理技術檔案中未針對這些先前事件識別出危害跡象，則基於所檢視的檔案，針對此新漏洞的已知未經身份驗證的利用路徑會在這些特定裝置上得到緩解。這並不能消除攻擊者持有有效netadmin憑證的風險。

Q:我是否可以親自執行驗證，而不是等待TAC?

A:無法共用管理技術的客戶可以執行附錄中描述的手動驗證步驟。結果是初步的；記錄調查結果並與TAC共用，TAC將執行正式評估。

Q:強化我的SD-WAN重疊的一般最佳實踐是什麼？

A:有關最佳實踐，請參閱Cisco Catalyst SD-WAN強化指南。

Q:Cisco TAC是否針對此漏洞提供取證分析或調查服務？

A:Cisco TAC可通過檢視PSIRT建議中記錄的危害表現的管理技術檔案來協助客戶。Cisco TAC不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，我們鼓勵客戶與其首選的第三方事件響應(IR)公司接洽。

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）。