

修正Catalyst SD-WAN安全建議 — 2026年9月

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[補救工作流程概述](#)

[步驟 1:從所有管理員收集管理技術檔案](#)

[替代方案：手動驗證（僅當無法收集管理技術時）](#)

[步驟 2:升級至固定軟體版本](#)

[步驟 3:開啟TAC案件並上傳管理技術檔案以進行掃描](#)

[步驟 4:如果識別出危害 — TAC指南](#)

[固定軟體版本](#)

[附錄:手動驗證步驟（僅當無法進行管理技術收集時）](#)

[如何確定危害表現](#)

[驗證 1:稽核服務代理訪問日誌](#)

[驗證 2:稽核Manager伺服器日誌](#)

[常見問題](#)

簡介

本文檔介紹根據PSIRT建議日期（2026年9月30日）識別和修復關鍵SD-WAN安全漏洞的步驟。思科強烈建議升級至固定軟體版本以修正此問題。

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（管理器、控制器和驗證器）
- Cisco Catalyst SD-WAN升級程式
- Cisco TAC案件管理和技術收集程式

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。

此建議可從以下連結獲得：

- [Cisco Catalyst SD-WAN Manager API身份驗證繞過](#)漏洞(CVE-2026-76504、CWE-177)。安全影響等級：關鍵 (CVSS基本分數9.8)。

此PSIRT建議解決了此缺陷：

- 思科錯誤ID [CSCww79570](#)

此建議會影響Cisco Catalyst SD-WAN Manager(vManage)。

補救工作流程概述



附註：所有運行早於第一個固定發行版的SD-WAN管理器(vManage)都易受攻擊，需要立即升級。但是，並非所有Catalyst管理器都顯示存在危害的證據。

所需操作：從所有Catalyst SD-WAN管理器收集管理技術，將所有升級為固定版本，然後開啟Cisco TAC案例，以便TAC掃描您的管理技術，發現危害跡象。

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 — 在所有Catalyst SD-WAN管理器(包括群集和災難恢復(DR)部署的每個節點)上運行管理技術，以確保不會丟失診斷資料。選擇「Log and Tech (日誌和技術選項)」。不需要核心。
 2. 升級到固定版本-將所有管理器(vManage)升級到「固定軟體版本」([Fixed Software Versions](#))表格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，請使用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:從所有管理員收集管理技術檔案

必需：在升級前從所有管理器(vManage)收集管理技術檔案，以確保不會丟失診斷資料。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. 對所有管理器運行管理技術(vManage)。
2. 如果您的管理器作為群集運行，請在每個群整合員上運行admin-tech。
3. 如果您部署了災難恢復(DR)，在主站點和災難恢復站點的每個Manager上運行管理技術。

[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:升級至固定軟體版本

在步驟1中收集管理技術後，將所有管理器(vManage)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。



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. 開啟標題為「CVE-2026-76504」的CVE-ID「CVE-2026-76504」的嚴重性3 TAC案例，以啟動掃描程式。
2. 上傳步驟1中收集的所有管理技術日誌捆綁包（所有管理器，包括群集和DR節點）。
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，則無需升級後執行進一步的操作。

步驟 4:如果識別出危害 — 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

這些軟體版本包含此漏洞的修補程式。升級至您目前版本系列中的第一個固定版本。

Cisco Catalyst SD-WAN軟體版本	第一個固定版本	可用軟體
20.91之前的版本 ^本	移轉至固定版本。	
20.9	20.9.10.1	適用於vManage的20.9.10.1升級映像
20.12	20.12.8.2	適用於vManage的20.12.8.2升級映像
20.15	20.15.6.1	適用於vManage的20.15.6.1升級映像

Cisco Catalyst SD-WAN軟體版本	第一個固定版本	可用軟體
20.18	20.18.4.1	適用於vManage的20.18.4.1升級映像
26.1	26.1.2.1	26.1.2.1適用於vManage的升級映像
26.2	26.2.1	26.2.1 vManage升級映像

¹這些版本已到達軟體維護結束。思科強烈鼓勵客戶升級至支援的版本。

思科產品安全事件響應團隊(PSIRT)僅驗證建議書中記錄的受影響和固定版本資訊。



附註：思科還已在基於雲的Cisco SD-WAN雲（思科託管）版本20.15.605中解決了此漏洞。無需使用者操作。客戶可以使用服務GUI中的「幫助」功能確定當前的補救狀態或軟體版本。

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:這些步驟必須在所有Manager(vManage)上執行，包括災難恢復(DR)站點中的每個群整合員和每個Manager。從vshell訪問日誌檔案(從Manager CLI訪問vshell)，並檢視當前日誌檔案和旋轉日誌檔案。

如何確定危害表現

該建議有兩個折中指標。兩者都與j_security_check的條目有關，其中請求的字元被編碼(例如/%6a_security_check)，來自未知或未經授權的IP地址。



重要：本節中的範例顯示使用%6a作為請求中的編碼字元j。這只是一個示例，該漏洞允許使用請求中編碼的任何一個字元。



附註：Cisco Catalyst SD-WAN Manager系統如果暴露於網際網路，且埠暴露於網際網路，則存在受到危害的風險。在某些情況下，這些危害表現會在標準操作期間出現。因此，必須根據正常的網路狀態評估它們以識別並避免誤報。

指示器	日誌檔案	它的含義	驗證
收到編碼的j_security_check請求	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	客戶端向Manager傳送了此類請求。	驗證 1
已為viptela-reserved-*使用者處理編碼的j_security_check請求	/var/log/nms/vmanage-server.log*	Manager處理了此型別的請求，該請求針對已保留的viptela-*使用者（已保留的系統服務帳戶）。	驗證 2

驗證 1:稽核服務代理訪問日誌

稽核位於/var/log/nms/containers/service_proxy/serviceproxy-access.log的serviceproxy-access.log檔案，以查詢與來自未知或未經授權的IP地址的j_security_check相關的條目，如以下示例所示：

[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168

vManage系統中的某些日誌檔案被限制在根訪問之後，客戶無法直接訪問。若要檢視這些日誌，客戶必須生成一個管理技術檔案。

解釋TAC的結果和檔案

如果沒有找到此類條目：

- 沒有在此管理器上的此日誌中檢測到危害跡象
- 記錄您的TAC案例的此結果
- 繼續驗證2，然後對其餘經理重複這兩個驗證

如果找到此類條目：

- 仔細檢查所示的每個源IP地址
- 查詢來自未知或未授權IP地址的條目。驗證源IP是否屬於環境中的授權活動（例如，運行的漏洞掃描或滲透測試）
- 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
- 包括日誌條目、時間戳、源IP和HTTP狀態代碼
- TAC執行正式評估確定

驗證 2:稽核Manager伺服器日誌

稽核位於/var/log/nms/vmanage-server.log的vmanage-server.log檔案，以查詢與來自未知或未授權IP地址的j_security_check相關的條目，特別是針對包含以viptela-reserved-開頭的名稱的使用者的呼叫，如下例所示：

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) [default] Request Store
```



附註：Viptela-reserved系統服務帳戶記錄在Cisco Catalyst SD-WAN系統和介面配置指南的身份驗證、授權和記賬部分。

解釋TAC的結果和檔案

如果沒有找到此類條目：

- 沒有在此管理器上的此日誌中檢測到危害跡象
- 記錄您的TAC案例的此結果
- 對其餘Manager重複上述兩種驗證

如果找到此類條目：

- 這可能表明存在潛在危害表現
 - 記錄所有調查結果並立即建立TAC案例
 - 包括案例中的日誌條目和時間戳，以及同一時間段的驗證1查詢結果
 - 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:從所有管理器收集管理技術檔案(vManage)，然後將所有管理器升級到固定軟體版本。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。

Q:哪些元件受此建議的影響？

A:僅影響Cisco Catalyst SD-WAN Manager(vManage)。

Q:我們是否還需要升級控制器、驗證器或邊緣路由器？

A:不，不是為了說明這個建議。將所有管理器(vManage)升級到固定版本，並使用[控制器相容性表](#)確認新Manager版本與其他元件相容。

Q:是否有變通辦法？

A:沒有。沒有解決此漏洞的解決方法。升級至固定版本。

Q:我需要升級到哪個版本？

A:儘快升級到當前版本系列中的第一個固定版本。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:我已升級到固定版本，以獲得先前的SD-WAN安全建議。我是否需要再次升級？

A:是，除非當前版本等於或晚於[固定軟體版本](#)表中的系列中第一個固定版本。早期建議中的固定版本不一定包含此漏洞的修復程式。

Q:我是否需要從所有經理那裡收集管理技術人員？

A:會。TAC需要來自每個Manager(vManage)的管理技術檔案，包括災難恢復(DR)站點中的每個群整合員和每個Manager，以便正確評估您的環境。

Q:我可以自己檢查危害表現嗎？

A:會。如果無法收集管理技術檔案，請在每個管理器上使用[手動驗證步驟](#)，並與TAC共用結果。管理員技術收集仍然是首選方法，TAC會做出正式評估決定。

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: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: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:我們是思科託管的重疊網路。我們是否需要檢查SSP上的任何訪問規則？

A:建議所有思科託管客戶在SSP > Overlay Details > Allow Inbound規則中檢視自己的允許入站規則，並確保僅允許來自您方所需的字首。這些規則僅用於管理訪問，不適用於邊緣路由器。

Q:Cisco TAC是否針對此漏洞提供取證分析或調查服務？

A:Cisco TAC可通過掃描與此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。

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）。