

檢查已有文章的粗體

目錄

[簡介](#)

[參考 — Cisco SD-WAN CVE-2026-L20182件](#)

[電子郵件](#)

[Sherlock 1 — 接收 — 請求升級和管理技術檔案](#)

[Sherlock 2 — 結果 — 未觀察到任何IoC \(每個檔案\)](#)

[Sherlock 3 — 提醒 — 缺少管理技術檔案](#)

[TAC 1 — 調查 — 需要進一步審查 \(懷疑IoC\)](#)

[TAC 2 — 結果 — 未找到IoC \(工程師確認\)](#)

[TAC 3 — 驗證 — 確認重疊中的IP所有權](#)

[TAC 4 — 結果 — 已清除誤報](#)

[TAC 5 — 嚴重 — 已識別IoC，安排複查呼叫](#)

[TAC 6 — 結果 — 重複IoC \(關閉並重新導向\)](#)

[TAC 7 — 修正 — 選項跟進 \(呼叫後\)](#)

[TAC 8 — 補救 — 受侵害交換矩陣的更新選項 \(選項2後續操作\)](#)

[TAC 17 — 反向查詢 — 以前沒有IoC，現在已標識IoC\(CVE-2026-20182\)](#)

[CloudOps 1 — 主動 — 在雲掃描中檢測到IoC，驗證需要管理技術](#)

[針對尚未完成選項A、B或C的先前受影響的客戶的WAVE 2A電子郵件。\(選項1和2需要重新完成\)](#)

[TAC 9模板，無適用於PSIRT2a的IOC/它們確實重建 \(先前受影響\)](#)

[TAC 10 Template for yes IOC for PSIRT2a/they done rebuild \(以前受影響\)](#)

[TAC 11模板，無適用於PSIRT2a的IOC/它們未重建 \(先前受影響\)](#)

[TAC 12 Template for yes IOC for PSIRT2a/they not rebuild\(PREVIOUS IMPACT\)](#)

[新客戶的WAVE 2A電子郵件 \(以前未受影響\)](#)

[TAC 13模板，無IOC/無可用的固定版本 \(WAVE 2a — 等待修復\)](#)

[無IOC/固定版本可用的TAC 14模板 \(WAVE 2a — 立即升級\)](#)

[TAC 15模板，用於IOC已識別/可用固定版本 \(WAVE 2a — 緊急升級\)](#)

[已識別IOC的TAC 16模板/無可用固定版本 \(WAVE 2a — 強化並等待修復\)](#)

簡介

本文檔集中了與Cisco Catalyst SD-WAN控制器身份驗證繞行漏洞相關的案例的分類和補救過程中使用的已批准客戶電子郵件模板。模板按發件人 — Sherlock (收集管理技術資料並返回初步IoC結果的自動案例交換) 和TAC工程師 (由人工驅動的後續調查、驗證和補救指南) 進行拆分。

參考 — Cisco SD-WAN CVE-2026-L20182件

以上電子郵件模板中引用的每個思科文檔的主清單。編號是統一的 — 每個郵件上標(例如^[2])指向此清單中的專案。

1. Cisco SD-WAN加固指南— <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. 正式安全建議(cisco-sa-sdwan-mltnps2-JxpWm7R)—
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. TAC修復指南 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-h1d--1516256622>
4. Cisco SD-WAN升級指南— <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. Cisco SD-WAN管理技術收集指南— <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. 第二個安全建議(cisco-sa-sdwan-rpa2-v69WY2SW)—
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. 開始Catalyst SD-WAN升級— <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

電子郵件

Sherlock 1 — 接收 — 請求升級和管理技術檔案

使用案例

為CVE-2026-20182開啟TAC案例，建議從收集管理技術資料，然後升級所有SD-WAN控制元件時進行初始推廣。

主題

重要：CVE-2026-20182 — 升級規劃和IoC評估所需操作

訊息

尊敬的客戶：

感謝您聯絡思科技術協助中心(TAC)。

有關CVE-2026-20182相關的漏洞，請檢視[官方安全建議](#)^[1]以瞭解全部詳細資訊以及TAC補救指南[\[2\]](#)。

我們的主要目標是幫助保護您的環境。請優先安排升級規劃和執行，將其作為降低此風險的最關鍵步驟。如果尚未計畫此升級，請立即執行此操作。

升級資源：有關如何執行升級的詳細說明，請參閱以下思科官方文檔：[Cisco SD-WAN升級指南](#)^[3]

要針對與CVE-2026-20182相關的任何潛在危害表現(loC)對您的環境進行初始評估，您必須在升級之前執行管理技術收集。請遵循以下操作順序：

1. **收集管理技術檔案：**在升級之前，從所有SD-WAN控制元件生成管理技術日誌，以確保不會丟失診斷資料。生成這些檔案時，請確保選擇「Logs」和「Tech」。
 - **vSmarts（控制器）：**一次收集一個，而不是同時收集。
 - **vBonds（驗證程式）：**從所有節點收集。
 - **管理器(vManage):**從群集中的所有節點（活動和備用DR）收集。
2. **執行升級：**將所有SD-WAN控制元件(vManage、vSmart、vBond)升級到顧問中列出的固定軟體版本。在開始升級之前，不要等待管理技術日誌分析，因為升級會立即關閉漏洞。
3. **上傳到TAC案例：**升級完成後，如有可能，將先前收集的檔案同時上傳到您的現有TAC案例。然後，我們的團隊將對這些日誌進行掃描，以評估您的環境中是否存在危害表現(loC)。

資源和支援：

有關生成和安全提交管理技術檔案的更多詳情和逐步說明，請參閱本指南：[Cisco SD-WAN管理技術收集指南](#)^[4]。

如果您訂有BCS/LCS，請聯絡Cisco NCE或Delivery Manager以獲得有關升級過程或後續步驟的其他指導。

您的資料隱私和安全仍然是我們的首要任務。提供的所有資訊都將根據思科的隱私和安全策略進行處理。

對於成功上傳到案例的每個檔案，您會收到自動電子郵件確認；請確保您檢視這些通知。

感謝您在保護基礎設施方面迅速合作。

連結：

[1] [官方安全諮詢](#)

[2] [TAC補救指南](#)

[3] [Cisco SD-WAN升級指南](#)

[4] [Cisco SD-WAN管理技術收集指南](#)

順祝商祺！

在Outlook中開啟

① 使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

Sherlock 2 — 結果 — 未觀察到任何IoC (每個檔案)

使用案例

在管理技術分析之後傳送的Sent顯示沒有觀察到特定上傳檔案的危害指標。每個處理檔案傳送一次。

主題

更新：SD-WAN元件[插入檔名] -CVE-2026-20182的分析結果

訊息

尊敬的客戶：

謝謝你的耐心。

我們已經完成了對admin-tech檔案[插入檔名]的分析。在該檔案中，我們沒有識別與此特定裝置的CVE-2026-20182相關的任何危害指標。

請注意，您檢索並提供給思科用於本次審查的日誌資料量可能受到您根據Cisco SD-WAN強化指南^[1]配置的日誌保留期的限制。

重要：後續步驟和案例結束：

1. **等待所有結果：**請注意，此電子郵件中的結果可能是部分結果。我們將分析提供的每個檔案。請等到收到所有上傳檔案的確認後，再考慮評估完成。
2. **升級優先順序：**雖然對管理技術日誌的初步掃描尚未識別出危害表現(IoC)，但底層漏洞可能仍然存在。對於Cisco Cloud-Pro和Cisco On-Prem部署，如果您尚未這樣做，請儘快確定您的SD-

WAN控制元件的完整升級的優先順序。

- Cisco Cloud(fka:SaaS)客戶交換矩陣由思科自動升級，作為託管服務的一部分。 無需任何操作。

3. **案例結束：**當您收到所有上傳檔案的「沒有觀察IoC」結果，並且（如果適用）已成功完成整個環境的軟體升級後，您可以考慮解決此問題並繼續執行標準關閉程式。

升級資源（如果適用）：有關如何執行Cisco Cloud-Pro和Cisco On-Prem升級的詳細說明，請參閱以下思科官方文檔：Cisco SD-WAN升級指南

升級過程的高級概述包括：

1. 將相應的軟體映像上傳到Manager(vManage)儲存庫。
2. 按順序升級控制器，從Manager(vManage)開始，然後是Validator(vBond)和Controller(vSmart)。
3. 啟用新軟體版本並驗證系統功能。

我們將繼續監視您的案例。如果在我們根據您提供的檔案提供了所有結果之後10個工作日內沒有收到回覆，我們將假定無需進一步的協助，並繼續進行正常的TAC案例關閉程式。如果您有任何需要，請通知我們。

順祝商祺！

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

Sherlock 3 — 提醒 — 缺少管理技術檔案

使用案例

提交的管理技術檔案與日誌中發現的SD-WAN控制元件數量不匹配時的自動跟蹤。

主題

提醒：CVE-2026-E評估所需的管理技術文20182丟失

訊息

尊敬的客戶：

您的SD-WAN控制元件中仍缺少管理技術，因此我們的系統無法從管理技術日誌評估任何危害指標。要開始CVE-2026-20182評估，我們必須從ALL Controllers(vSmarts)、Validators(vBonds)和Managers(vManage)接收管理技術檔案，包括群集時的所有Manager(vManage)節點。

後續步驟：

請儘快上傳其餘的管理技術檔案。

順祝商祺！

在Outlook中開啟

①傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (帶正文)

↓ Download .eml Template

TAC 1 — 調查 — 需要進一步審查 (懷疑IoC)

使用案例

自動化程式發現可能危害的日誌後，由TAC工程師傳送，需要人工調查。

主題

SR # — 需要進一步調查

訊息

尊敬的客戶：

我的名字是{your_name}，我接受了您的案例。感謝您繼續與思科技術協助中心(TAC)合作。

在對您從SD-WAN控制元件提供的管理技術檔案進行初步分析後，我們確定需要進行TAC進一步調查才能完成我們的分析。為了幫助確保徹底而準確地解決問題，我將與您密切合作，執行後續步驟。

請放心，我們將致力於支援您完成這些後續步驟，並將提供明確的指導，以便有效處理這一情況。

請確定升級規劃和執行的優先順序，將其作為降低此風險的最關鍵步驟。如果尚未計畫此升級，請立即執行此操作。

如果您有任何問題或需要幫助，請隨時聯絡您的TAC工程師。

感謝您的關注和合作。

順祝商祺！

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (帶正文)

↓ Download .eml Template

TAC 2 — 結果 — 未找到IoC (工程師確認)

使用案例

自動化功能未找到任何危害表現且工程師已確認結果後，由TAC工程師傳送。

主題

更新：TAC稽核完成 — 未找到CVE-2026-20182的IoC — 案例[SR #]

訊息

您好，[客戶姓名]

我是Cisco TAC工程師，指定給您的案例[SR Number]。

對您從SD-WAN控制元件提供的管理技術檔案執行初步掃描後，我們找不到與思科SD-WAN安全諮詢中描述的危害指示符一致的日誌條目：

- Cisco Catalyst SD-WAN控制器驗證旁路漏洞[1]

- Cisco Catalyst SD-WAN管理器漏洞[2]

但是，您應該繼續將所有SD-WAN控制元件升級到<insert version>。 以下是繼續升級的步驟：

- 啟動Catalyst SD-WAN升級[3]
- Cisco SD-WAN升級指南[4]

請注意，由於Internet上IP編址的動態性質，以及我們缺乏對客戶網路中邊緣裝置的預期IP地址的瞭解，思科無法評估邊緣裝置的日誌。我們鼓勵客戶遵循Cisco Catalyst SD-WAN控制器身份驗證繞行漏洞安全建議中所述的對等事件驗證指南，手動完成此步驟。 此外，還鼓勵客戶完成與對等事件驗證相關的其他檢測步驟，如針對CVE-2026-20182的安全建議中所述。

連結

[1] Cisco Catalyst SD-WAN控制器身份驗證旁路漏洞 —

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Cisco Catalyst SD-WAN管理器漏洞 —

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3]開始Catalyst SD-WAN升級 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Cisco SD-WAN升級指南 — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

此致，

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 3 — 驗證 — 確認重疊中的IP所有權

使用案例

TAC工程師傳送此郵件，詢問客戶在日誌分析過程中出現的特定IP地址是屬於還是屬於其SD-WAN重疊基礎架

構的一部分。

主題

[SR #] — 需要IP地址驗證

訊息

尊敬的[客戶名稱]:

我是[您的姓名]，是您的案例的Cisco TAC工程師。

作為我們持續分析您從SD-WAN控制元件提供的管理技術檔案的一部分，我們需要您幫助驗證以下IP地址是否屬於或曾經屬於您的SD-WAN重疊基礎架構：

有問題的IP地址：

- [IP地址1]

- [IP地址2]

為了幫助我們完成評估，請確認：

- 1.此IP地址當前是否與SD-WAN重疊中的任何元件（如vManage、vSmart、vBond或邊緣裝置）相關聯？
- 2.此IP地址以前是否曾被任何可能已經停用或其IP已更改的SD-WAN控制元件使用？
- 3.此IP是否與災難恢復(DR)站點或與您的SD-WAN部署相關的任何其他基礎設施相關聯？

你方迅速反應將讓我們繼續進行分析，並向你方提供接下來的適當步驟。

如果您有任何問題，請隨時聯絡。

順祝商祺！

在Outlook中開啟

①傳送前替換所有[括弧中的佔位符]。

✉ Open Outlook (帶正文)

↓ Download .eml Template

使用案例

手動稽核確定自動掃描標籤的初始IoC為誤報後，由TAC工程師傳送。

主題

更新：CVE-2026-20182技術審查 — 案例[案例號]

訊息

尊敬的客戶：

感謝您在工程團隊手動稽核您從SD-WAN控制元件提供的管理技術檔案的過程中耐心等待。

經過徹底調查，我們已確定我們的自動掃描流程所標籤的初始危害表現(IoC)為誤報，即我們的評估是IoC無效。

重要：當此特定警報已被清除時，請注意，與[CVE-2026-20182](#)[1]相關的漏洞需要升級軟件，以幫助確保SD-WAN交換矩陣的長期安全性和完整性。

如果您尚未完成升級：請儘快確定您的SD-WAN控制元件全面升級的優先順序。升級是有效修復此漏洞的唯一方式。有關詳細說明，請參閱[Cisco SD-WAN升級指南](#)[2]。

如果您已完成升級：由於我們已將此調查結果確認為假陽性，並且您已經執行了軟體補救，因此無需執行進一步操作。您可以認為此問題已解決，並繼續執行標準關閉過程。

感謝您在確定基礎設施安全優先順序方面盡心盡力。如果您有任何進一步的問題或需要額外幫助，請立即聯絡我們。

順祝商祺！

思科技術支援中心(TAC)

連結：

[1] [官方安全諮詢](#)

[2] [Cisco SD-WAN升級指南](#)

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

使用案例

TAC工程師在確認潛在危害表現時傳送，並且需要緊急客戶呼叫討論發現結果和後續步驟。

主題

緊急：CVE-2026-2010的分析結果20182確定危害指標

訊息

尊敬的客戶：

感謝您耐心等待我們分析為SD-WAN控制元件提供的管理技術檔案。

通過技術審查，我們確定了與CVE-2026-20182相關的潛在危害指標(LoC)。

鑑於這些調查結果的性質，我們必須儘快討論技術細節和建議的後續步驟。我們希望安排與您的團隊進行電話聯絡，以審查具體調查結果並討論適當的補救措施。

後續步驟：

- **安排會議:**請在接下來的[例如4-8小時]內向我們通報您是否有空來檢視這些調查結果。
- **升級SDWAN控制元件:**請儘快將您的SDWAN管理器、控制器和驗證器升級到固定版本。

我們的主要目標是幫助您保護您的環境並降低任何潛在風險。感謝你方迅速關注此事，並期待與你協調。

順祝商祺！

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (帶正文)

↓ Download .eml Template

TAC 6 — 結果 — 重複LoC (關閉並重新導向)

使用案例

當LoC分析確認發現與同一客戶/環境的早期SR相匹配時，由TAC工程師傳送。當前案例已關閉，且客戶被重新定向到已提供補救指導的原始SR。

主題

更新：CVE-2026-20182技術審查 — 案例[SR #]（確認重複IoC）

訊息

尊敬的客戶：

感謝您耐心等待我們分析為SD-WAN控制元件提供的管理技術檔案。我們確定，我們的掃描進程所標籤的初始危害表現(IoC)與已在[原始SR #]中傳送的**初始指標相同**。如前所述，我們建議緊急升級，並按照[TAC修正指南](#)^[2]中概述的兩個補救路徑之一繼續進行，以儘快保護您的環境。有關完整[詳細資訊，請參閱 CVE-2026-20182](#)^[1]的官方安全建議。

現在我要結束這個案子。請使用[原始SR編號]請求有關升級或補救的進一步指南或技術支援。

順祝商祺！

[您的姓名]

連結：

[1]官 [方安全諮詢](#)

[2] TAC [補救指南](#)

在Outlook中開啟

① 傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (帶正文)

↓ Download .eml Template

TAC 7 — 修正 — 選項跟進 (呼叫後)

使用案例

在IoC審閱呼叫後傳送，以重新顯示所討論的補救路徑。客戶選擇選項A (通過滾動重啟重新部署)、選項B (通過硬切換重新部署) 或選項C (完整系統重建)。

主題

跟進：CVE-2026-20182的補救選項

訊息

尊敬的客戶：

感謝您花時間討論我們最近分析的結果。正如我們在上次呼叫中討論的那樣，我們建議繼續使用以下補救路徑之一來保護您的環境。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明：涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明：涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項 C：完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要具備重建模板和策略資料庫的專業知識。

後續步驟：

- 請在內部討論這些選項，並讓我們知道您打算採取哪條路徑。一旦您做出決定，我們可提供進一步的指導或技術支援，以協助您度過執行階段。

我們在此支援您完成整個過程。如果您對這些選項有任何疑問，請通知我們。

順祝商祺！

思科技術支援中心(TAC)

附註：選項1是升級。認為此升級已執行的方案。

在Outlook中開啟

① 使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 8 — 補救 — 受侵害交換矩陣的更新選項 (選項2後續操作)

使用案例

通知其SD-WAN交換矩陣遭到破壞且以前追求的選項2，以及認為其交換矩陣仍存在威脅實施者永續性的風險的客戶。重建受損交換矩陣（並且不依賴於備份/現有configDB）的客戶不會面臨風險，也不會收到此通訊。該通訊內容將由TBD傳送。

主題

需要採取緊急行動：SD-WAN基礎設施關鍵漏洞補救

訊息

尊敬的客戶：

我們將提供關鍵更新，以補救您的SD-WAN交換矩陣，如[SR#]和以前通報的安全公告中所述。此更新特定於所提供日誌顯示危害表現(IOC)證據的交換矩陣。

雖然您之前選擇了基於選項2的補救計畫（包括軟體升級、控制器重新部署和SSH金鑰輪替），我們對威脅情況的分析仍在不斷發展。關於利用這些漏洞的新技術見解表明，強烈敦促採取更多措施，以降低永續性風險，並幫助確保證書信任鏈的完整性。

所需操作：

我們更新了推薦的補救策略，通過包括額外的根證書輪換來提供更全面的防禦。

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。

鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明:涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明:涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項C:完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並

且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要具備重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您需要在我們的技術支援中心(TAC)開具服務請求(SR)，請告知我們是否需要進一步的技術說明。

此致，
Cisco

在Outlook中開啟

① 使用下面的 .eml 下載。傳送前替換所有 [帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 17 — 反向查詢 — 以前沒有IoC，現在已標識IoC(CVE-2026-20182)

使用案例

傳送給以前通知未發現危害指標(IoC)的客戶，但隨後對管理技術日誌的內部稽核已發現與CVE-2026-20182相關的IoC的客戶。傳達修改後的發現並提供三個補救選項(選項A、B或C)。

主題

重要更新：CVE-2026-20182的修訂版IoC評估 — 現已確定危害指標 — SR [SR#]

訊息

尊敬的客戶：

感謝您繼續與思科技術支援中心(TAC)就服務請求[SR#]項下的CVE-2026-20182開展合作。

在我們之前的通訊中，我們建議我們對從您的SD-WAN控制元件提供的管理技術檔案的分析未發現與此建議相關的任何危害表現(IoC)。作為我們對您的安全持續承諾的一部分，自那以後，我們對與您的組織交換矩陣相關的其他管理技術日誌資料進行了例行內部稽核。

此後的審查確定了初次評估期間未出現的危害指標(loC)。我們正在與您合作解決這些發現問題。這些 loC 指示組織交換矩陣中可能的可疑活動，從而保證採取補救措施。

我們認識到這將修改以前向您傳送的結果，並且我們希望確保您清楚準確地瞭解您的環境，以便進行適當的補救。

所需操作：

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。

鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明：涉及控制器重新部署，以及 SSH 金鑰和證書輪替。在遷移過程中，通過 vManage 連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明：涉及控制器重新部署以及 SSH 金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項 C：完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您希望通過回覆本電子郵件或通過我們的技術支援中心(TAC)的現有服務請求(SR)進一步獲得技術說明，請通知我們。

此致，
Cisco

①使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

CloudOps 1 — 主動 — 在雲掃描中檢測到IoC，驗證需要管理技術

使用案例

當雲託管SD-WAN交換矩陣的思科CloudOps安全掃描出現潛在危害表現(IoC)時，主動傳送。系統會代表客戶開啟SR，並要求客戶附加管理技術檔案，以便通過完整的日誌分析來驗證調查結果。

主題

需採取的行動：驗證安全掃描查詢結果所需的管理技術檔案 — SR [SR#]

訊息

尊敬的客戶：

作為我們持續致力於保護和監控思科產品完整性的部分內容，思科最近完成了特定雲託管SD-WAN交換矩陣的安全掃描。這一行動是為了應對所報告的安全關切。掃描已識別出組織交換矩陣中可能的可疑活動，需要進一步審查。

我們請求您協助將管理技術檔案附加到代表您開啟的此服務請求(SR)，以便我們能夠驗證此發現並完成我們的調查。

要啟用完整分析，請收集並上傳所有SD-WAN控制元件中的管理技術檔案。生成這些檔案時，請確保選擇「日誌」和「技術」：

- **vSmarts (控制器)**：一次收集一個，而不是同時收集。
- **vBonds (驗證程式)**：從所有節點收集。
- **管理器(vManage)**:從群集中的所有節點 (活動和備用DR) 收集。

有關生成和安全提交管理技術檔案的詳細分步說明，請參閱本指南：[Cisco SD-WAN管理技術收集指南](#)^[1]。

收到請求的檔案後，我們的團隊將對其進行分析，確認觀察到的活動是否代表真正的危害表現，並且就適當的後續步驟為您提供建議。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您在回覆本服務請求(SR)時需要進一步的技術澄清，請通知我們。

順祝商祺！

Cisco

連結：

[1] [Cisco SD-WAN管理技術收集指南](#)

在Outlook中開啟

① 使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

針對尚未完成選項A、B或C的先前受影響的客戶的WAVE 2A電子郵件。（ 選項1和2需要重新完成 ）

TAC 9模板，無適用於PSIRT2a的IOC/它們確實重建(先前受影響)

使用案例

傳送給其SD-WAN日誌未顯示與PSIRT2a建議和PSIRT先前重建交換矩陣的危害表現(IoC)的客戶。提供更新的補救指南，提供三個選項（ 選項2的後續選項 ）。

主題

需要採取緊急行動：SD-WAN基礎設施關鍵漏洞補救 — SR [SR#]

訊息

尊敬的客戶：

感謝您就服務請求[SR#]下最近的SD-WAN PSIRT建議與思科技術支援中心(TAC)聯絡。

在檢視您的SD-WAN交換矩陣中提供的日誌和資訊後，我們的分析未確定與2026年6月5日SD-WAN漏洞諮詢相關的任何危害指標(IoC)。此外，我們瞭解您的環境之前已進行了重建，這是與早期建議相關的補救措施的一部分。

考慮到與這些漏洞相關的最新發現，我們希望分享有關針對SD-WAN交換矩陣的建議補救指南的重要更新。

我們將提供關鍵更新，以補救您的SD-WAN交換矩陣，如[SR#]和以前通報的安全公告中所述。

雖然您之前選擇了基於選項2的補救計畫（包括軟體升級、控制器重新部署和SSH金鑰輪替），我們對威脅情況的分析仍在不斷發展。關於利用這些漏洞的新技術見解表明，強烈敦促採取更多措施，以降低永續性風險，並幫助確保證書信任鏈的完整性。

所需操作：

我們更新了推薦的補救策略，通過包括額外的根證書輪換來提供更全面的防禦。

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明：涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明：涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項C：完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您希望通過回覆此電子郵件或通過現有服務請求進一步進行技術說明，請通知我們。

此致，
Cisco

在Outlook中開啟

①使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 10 Template for yes IOC for PSIRT2a/它們確實重建(以前受到影響)

使用案例

傳送給其SD-WAN日誌顯示與PSIRT2a建議相關的**危害表現(IoC)**以及**先前重建交換矩陣**的客戶。提供更新的補救指南，提供三個選項（選項2的後續選項）。

主題

需要採取緊急行動：SD-WAN基礎設施關鍵漏洞補救 — SR [SR#]

訊息

尊敬的客戶：

感謝您就服務請求[SR#]下最近的SD-WAN PSIRT建議與思科技術支援中心(TAC)聯絡。

在分析您的SD-WAN交換矩陣提供的日誌後，我們的團隊確定了2026年6月5日SD-WAN漏洞諮詢的相關危害指標(IoC)。我們還瞭解您的環境之前已進行了重建，作為與早期建議相關的補救步驟的一部分。

我們將提供關鍵更新，以補救您的SD-WAN交換矩陣，如[SR#]和以前通報的安全公告中所述。此更新特定於所提供日誌顯示危害表現(IoC)證據的交換矩陣。

雖然您之前選擇了基於選項2的補救計畫（包括軟體升級、控制器重新部署和SSH金鑰輪替），我們對威脅情況的分析仍在不斷發展。關於利用這些漏洞的新技術見解表明，強烈敦促採取更多措施，以降低永續性風險，並幫助確保證書信任鏈的完整性。

所需操作：

我們更新了推薦的補救策略，通過包括額外的根證書輪換來提供更全面的防禦。

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程

中存在殘餘的威脅持續風險。

說明:涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明:涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項C:完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您希望通過回覆此電子郵件或通過現有服務請求進一步進行技術說明，請通知我們。

此致，
Cisco

在Outlook中開啟

①使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 11模板，無適用於PSIRT2a的IOC/它們未重建(以前 **受到影響**)

使用案例

傳送給其SD-WAN日誌未顯示與PSIRT2a建議相關的危害表現(IoC)且未重新構建交換矩陣的客戶。提供更新的補救指南，提供三個選項 (選項1的後續選項) 。

主題

需要採取緊急行動：SD-WAN基礎設施關鍵漏洞補救 — SR [SR#]

尊敬的客戶：

感謝您就服務請求[SR#]下最近的SD-WAN PSIRT建議與思科技術支援中心(TAC)聯絡。

在檢視您的SD-WAN交換矩陣提供的日誌和資訊後，我們沒有確定與2026年6月5日SD-WAN漏洞諮詢相關的危害表現(IOC)。

我們還知道，您的環境尚未根據前面的指導進行完全重建。思科建議檢視以下更新的補救指南，以幫助降低潛在風險，並增強SD-WAN證書信任鏈的完整性。

考慮到這一點，我們正在提供關鍵更新，以補救您的SD-WAN交換矩陣，如[SR#]和以前通報的安全公告中所述。

雖然您之前選擇了基於選項1（結合軟體升級和SSH金鑰輪替）的補救計畫，我們對威脅情況的分析仍在不斷發展。關於利用這些漏洞的新技術見解表明，強烈敦促採取更多措施，以降低永續性風險，並幫助確保證書信任鏈的完整性。

所需操作：

我們更新了推薦的補救策略，通過包括額外的根證書輪換來提供更全面的防禦。

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明:涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明:涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項C:完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您希望通過回覆此電子郵件或通過現有服務請求進一步進行技術說明，請通知我們。

此致，
Cisco

在Outlook中開啟

① 使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 12 Template for yes IOC for PSIRT2a/they not rebuild(先前受**影響**)

使用案例

傳送給其SD-WAN日誌顯示與PSIRT2a建議相關的**危害表現(IoC)**且**未重新構建其交換矩陣**的客戶。提供更新的補救指南，提供三個選項（選項1的後續選項）。

主題

需要採取緊急行動：SD-WAN基礎設施關鍵漏洞補救 — SR [SR#]

訊息

尊敬的客戶：

感謝您就服務請求[SR#]下最近的SD-WAN PSIRT建議與思科技術支援中心(TAC)聯絡。

在分析您的SD-WAN交換矩陣提供的日誌後，我們的團隊確定了2026年6月5日SD-WAN漏洞諮詢的相關危害指標(IoC)。此外，我們瞭解您的環境尚未根據先前的建議進行完全重建。

鑑於這些指標的存在和對威脅形勢的不斷瞭解，必須稽核並實施下面概述的更新補救指南，以降低持續存在的風險，並確保您的SD-WAN證書信任鏈的完整性。

我們將提供關鍵更新，以補救您的SD-WAN交換矩陣，如[SR#]和以前通報的安全公告中所述。此更新

特定於所提供日誌顯示危害表現(IOC)證據的交換矩陣。

雖然您之前選擇了基於選項1（結合軟體升級和SSH金鑰輪替）的補救計畫，我們對威脅情況的分析仍在不斷發展。關於利用這些漏洞的新技術見解表明，強烈敦促採取更多措施，以降低永續性風險，並幫助確保證書信任鏈的完整性。

所需操作：

我們更新了推薦的補救策略，通過包括額外的根證書輪換來提供更全面的防禦。

請注意，修正將有必要進行額外的維護活動，其中可能包括計畫內網路停機時間。鑑於我們的優先任務是確保您網路的安全性和完整性，我們開發了三種不同的補救方案。以下每個選項均提供操作影響與安全保證之間的平衡，供您考慮。由於您的內部風險狀況是獨一無二的，思科無法建議特定路徑。

選項 A：使用滾動重啟重新部署。通過避免網路停機來排定運營連續性的優先順序，不過在過渡過程中存在殘餘的威脅持續風險。

說明:涉及控制器重新部署，以及SSH金鑰和證書輪替。在遷移過程中，通過vManage連線現有控制器元件以部署新交換矩陣，然後在裝置遷移後立即刪除每個控制器元件。

選項 B：通過硬轉換重新部署。提供更高級別的安全保證。由於新控制器永遠不會連線到舊控制器，因此會進行完全隔離。由於所有裝置都需要重新建立連線並交換路由/連線資訊，因此這會對整體網路運營造成影響。中斷時間將取決於站點數量、交換的字首數量等。

說明:涉及控制器重新部署以及SSH金鑰和證書輪替，但在重新部署期間，舊控制器元件與新交換矩陣隔離。

選項C:完全重建系統。通過建立乾淨的基線來提供最高級別的安全保證，儘管這是最複雜的方法，並且在重建期間存在與配置相關的更高不穩定風險。這是一個漫長的選擇，需要重建模板和策略資料庫的專業知識。

在您的團隊審閱了這些選項並確定了與您的風險管理標準最相符的方法之後，請回覆此郵件以通知我們。收到您的選擇後，我們將協調維護視窗，開始執行所需的技術準備。

感謝您一如既往地專注於維護安全的網路基礎設施。如果您希望通過回覆此電子郵件或通過現有服務請求進一步進行技術說明，請通知我們。

此致，
Cisco

①使用下面的 .eml 下載。傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

新客戶的WAVE 2A電子郵件 (以前未受影響)

TAC 13模板，無IOC/無可用的固定版本 (WAVE 2a — 等待修復)

使用案例

傳送給其SD-WAN日誌未顯示與CVE-2026-20245相關的**危害指標(IoC)**，但其平台/版本目前沒有固定軟體版本的客戶。建議客戶應用臨時強化措施並等待固定版本通知。

主題

更新：完成CVE-2026-20245的IoC評估 — 當前無固定版本 — SR [SR#]

訊息

尊敬的客戶：

感謝您根據服務請求[SR#]聯絡思科技術支援中心(TAC)就CVE-2026-20245進行聯絡。

我們已經完成了對您從SD-WAN控制元件提供的管理技術檔案的分析。**在稽核的日誌中，我們沒有發現與CVE-2026-20245相關的任何危害表現(IoC)。**

請注意，根據[Cisco SD-WAN強化指南](#)^[1]在環境中配置的日誌保留期，可能會限制檢索並提供給思科進行本次審查的日誌資料量。

重要資訊 — 當前沒有可用的固定軟體版本：

目前，您的當前平台和軟體版本沒有可用的固定軟體版本來修補此漏洞。思科工程部門正在積極致力於提供固定版本。一旦固定軟體可用，將使用[固定版](#)^{本資訊}更新官方安全建議[2]。

建議採取的臨時措施：

在等待固定版本時，我們強烈建議實施以下強化措施以減少您的暴露風險：

1. **應用強化最佳實踐**：檢視並實施[Cisco SD-WAN強化指南](#)^[1]中的建議，以減少攻擊面。
2. **監控資安顧問諮詢**：定期檢視官[方安全諮詢](#)^[2]以了解有關您的平台固定版本可用性的更新。
3. **升級計畫**：立即開始您的升級計畫，以便在發佈固定版本後立即執行升級。
4. **監控您的環境**：繼續監控SD-WAN控制元件以發現任何異常行為或意外配置更改。

後續步驟：

當固定軟體版本可用時，我們將更新此案例。此時，您應該確定所有SD-WAN控制元件(Manager、Controller、Validator)儘快升級到固定版本的優先順序。

如果您有BCS/LCS訂用，請聯絡Cisco NCE或Delivery Manager以獲得有關升級計畫的更多指導。

感謝您的耐心和對基礎設施安全的承諾。如果您在案件審理過程中有任何問題或需要進一步的協助，請立即對本案作出答覆。

順祝商祺！

思科技術支援中心(TAC)

連結：

[1] [Cisco SD-WAN加固指南](#)

[2]官[方安全建議\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

在Outlook中開啟

①傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

無IOC/固定版本可用的TAC 14模板 (WAVE 2a — 立即升級)

使用案例

傳送給其SD-WAN日誌未顯示與CVE-2026-20245相關的危害表現(IoC)且有固定軟體版本的客戶。建議客戶立即繼續進行升級規劃和執行。

主題

更新：完成CVE-2026-20245的IoC評估 — 未找到IoC，需要升級 — SR [SR#]

訊息

尊敬的客戶：

感謝您根據服務請求[SR#]聯絡思科技術支援中心(TAC)就CVE-2026-20245進行聯絡。

我們已經完成了對您從SD-WAN控制元件提供的管理技術檔案的分析。在稽核的日誌中，我們沒有發現與CVE-2026-20245相關的任何危害表現(LoC)。

請注意，根據[Cisco SD-WAN強化指南](#)^[1]在環境中配置的日誌保留期，可能會限制檢索並提供給思科進行本次審查的日誌資料量。

重要 — 需要升級：

雖然未發現任何LoC，但是在SD-WAN控制元件升級到固定軟體版本之前，底層漏洞仍然存在。現在，您的平台可使用固定版本。

請優先確定升級規劃和執行的優先順序，將其作為補救此漏洞的最關鍵步驟。如果尚未計畫此升級，請立即執行此操作。

後續步驟：

1. **升級所有SD-WAN控制元件：**將Manager(vManage)、Controller(vSmart)和Validator(vBond)升級到官方安全建議^[2]中列出的固定軟體版本。
2. **升級資源：**有關詳細的升級說明，請參閱以下思科官方文檔：
 - [啟動Catalyst SD-WAN升級](#)^[3]
 - [Cisco SD-WAN升級指南](#)^[4]
3. **案例結束：**成功完成整個環境的軟體升級後，可以考慮解決此問題並繼續執行標準關閉過程。

如果您有BCS/LCS訂用，請聯絡Cisco NCE或Delivery Manager以獲得有關升級過程的更多指導。

我們將繼續監視您的案例。如果在10個工作日內沒有收到回覆，我們將假定無需進一步協助，並進入正常的TAC案例解決程式。

順祝商祺！

思科技術支援中心(TAC)

連結：

[1] [Cisco SD-WAN加固指南](#)

[2] 官方安全建議([cisco-sa-sdwan-privesc-4uxFrdzx](#))

[3] [開始Catalyst SD-WAN升級](#)

[4] [Cisco SD-WAN升級指南](#)

在Outlook中開啟

①傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

TAC 15模板，用於IOC已識別/可用固定版本 (WAVE 2a — 緊急升級)

使用案例

傳送給其SD-WAN日誌顯示與CVE-2026-20245相關的危害表現(IoC)且有固定軟體版本可用的客戶。建議客戶緊急升級，並安排審查電話討論結果和補救。

主題

緊急：已確定CVE-2026-20245的IoC — 需要立即升級 — SR [SR#]

訊息

尊敬的客戶：

感謝您根據服務請求[SR#]聯絡思科技術支援中心(TAC)就CVE-2026-20245進行聯絡。

通過分析您的SD-WAN控制元件提供的管理技術文件，我們的團隊已識別出與CVE-2026-E關聯的危害表現(IoC20245)。

鑑於這些調查結果的性質，我們必須儘快討論技術細節和建議的後續步驟。我們希望安排與您的團隊進行電話聯絡，以審查具體調查結果並討論適當的補救路徑。

需要立即執行的操作：

1. **立即升級SD-WAN控制元件：**您的平台可使用固定軟體版本。請儘快將Manager(vManage)、Controller(vSmart)和Validator(vBond)升級到官方安全建議^[1]中列出的固定軟體版本。升級會立即關閉漏洞。
2. **安排稽核呼叫：**請在接下來的[例如4-8小時]內向我們通報您是否有時間進行簡短通話，以檢視IoC調查結果並討論建議的補救選項。
3. **應用強化最佳實踐：**檢視並實施[Cisco SD-WAN加固指南](#)^[2]中的建議，以在規劃補救時減少攻擊面。

升級資源：

- [啟動Catalyst SD-WAN升級](#)^[3]

- [Cisco SD-WAN升級指南](#)^[4]

重要：升級後，可能會建議其他補救步驟（例如控制器重新部署和證書輪替），具體取決於所識別威脅的嚴重性。這些將在審查電話會議上討論。

另請參閱[TAC修正指南](#)^[5]以了解詳細修正選項。

我們的主要目標是幫助您保護您的環境並降低任何潛在風險。感謝你方迅速關注此事，並期待與你協調。

順祝商祺！

思科技術支援中心(TAC)

連結：

[1]官 [方安全建議\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Cisco SD-WAN加固指南](#)

[3][開始Catalyst SD-WAN升級](#)

[4] [Cisco SD-WAN升級指南](#)

[5] TAC[補救指南](#)

在Outlook中開啟

①傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

已識別IOC的TAC 16模板/無可用固定版本（WAVE 2a — 強化並等待修復）

使用案例

傳送給其SD-WAN日誌顯示與CVE-2026-20245相關的**危害指標(IoC)的客戶**，但這些客戶當前沒有適用於其平台/版本的**固定軟體版本**。建議立即強化、安排審查呼叫，並通知客戶他們必須等待固定版本才能完全補救。

主題

緊急：已標識CVE-2026-20245的IoC — 當前無固定版本 — SR [SR#]

訊息

尊敬的客戶：

感謝您根據服務請求[SR#]聯絡思科技術支援中心(TAC)就CVE-2026-20245進行聯絡。

通過分析您的SD-WAN控制元件提供的管理技術文件，我們的團隊已識別出與CVE-2026-E關聯的危害表現(IoC20245)。

鑑於這些調查結果的嚴重性，我們儘快討論技術細節和建議採取臨時措施至關重要。我們希望與您的團隊安排一次電話會議，以審查具體的調查結果。

重要資訊 — 當前沒有可用的固定軟體版本：

目前，沒有適用於您當前平台的固定軟體版本和軟體版本來完全修補此漏洞。思科工程部門正在積極致力於提供固定版本。一旦固定軟體可用，將使用[固定版本](#)^{本資訊更新}官方安全建議[1]。

需要立即執行的操作：

1. **安排稽核呼叫：**請在接下來的[例如4-8小時]內向我們通報您是否有時間進行簡短通話，以檢視IoC調查結果並討論臨時遏制措施。
2. **立即應用強化最佳實踐：**檢視並實施[Cisco SD-WAN強化指南](#)^[2]中的建議，以縮短攻擊面，同時等待固定版本。
3. **加強監控：**密切監視您的SD-WAN控制元件，以瞭解任何異常行為、意外配置更改或未經授權的訪問嘗試。
4. **監控資安顧問諮詢：**定期檢視官[方安全諮詢](#)^[1]以了解有關您的平台固定版本可用性的更新。
5. **升級計畫：**立即開始您的升級計畫，以便在發佈固定版本後立即執行升級。

後續步驟：

當固定軟體版本可用時，我們將更新此案例。此時，您必須確定所有SD-WAN控制元件（管理器、控制器、驗證器）立即升級到固定版本的優先順序。升級後，將根據我們通話期間檢查的發現討論其他補救步驟（如控制器重新部署和證書輪換）。

另請參閱[TAC修正指南](#)^[3]以瞭解固定版本可用後將會應用的修正選項的相關資訊。

我們的主要目標是幫助您保護您的環境並降低任何潛在風險。感謝你方迅速關注此事，並期待與你協調。

順祝商祺！

思科技術支援中心(TAC)

連結：

[1]官 [方安全建議\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Cisco SD-WAN加固指南](#)

[3] TAC [補救指南](#)

在Outlook中開啟

①傳送前替換所有[帶括弧的佔位符]。

✉ Open Outlook (僅主題)

↓ Download .eml Template

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）。