更新DNS Umbrella證書以在2024年10月生效

目錄

[簡介](#)

[背景資訊](#)

[瑕疵資訊](#)

[固定已核發](#)

- [CCO版本](#)

[修正矩陣](#)

- [1. 在控制器模式下運行Cisco IOS XE軟體版本17.5.x或更早版本的思科裝置](#)
  - [自動](#)
  - [手動](#)
- [2. 在控制器模式下運行Cisco IOS XE軟體版本17.6.x到17.8.x的Cisco裝置](#)
  - [自動](#)
  - [手動](#)
- [3. 在控制器模式下運行Cisco IOS XE軟體版本17.9.5a的思科裝置](#)
- [4. 在控制器模式下運行Cisco IOS XE軟體版本17.9.6的Cisco裝置](#)
- [5. 在控制器模式下為Cisco IOS XE軟體版本17.12.3a的思科裝置](#)
- [6. 在控制器模式下運行Cisco IOS XE軟體版本17.12.4的思科裝置](#)

簡介

本文檔介紹如何解決SD-WAN路由器使用過期證書而不是新證書的DNS Umbrella問題。

背景資訊

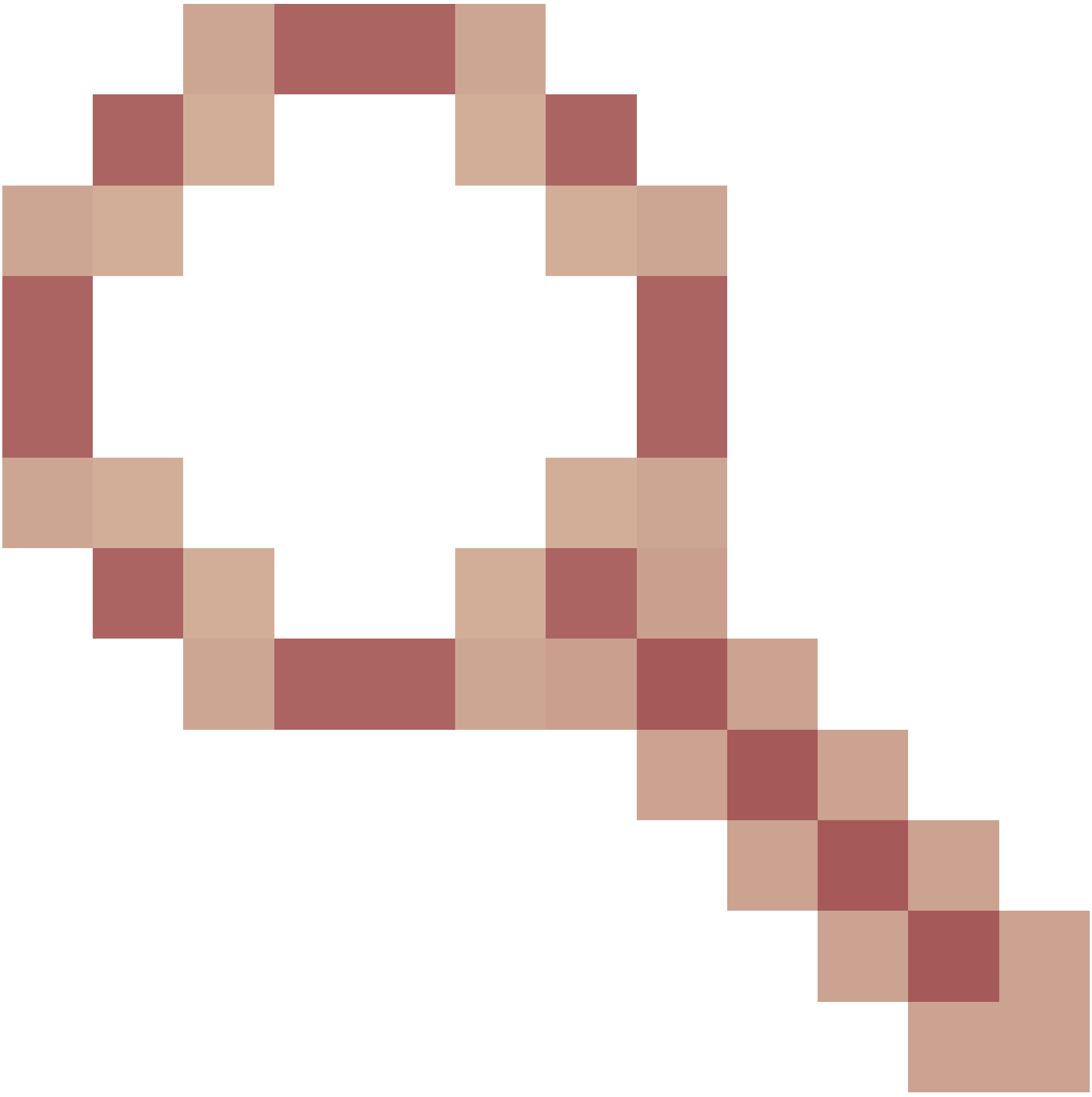
Cisco Catalyst SD-WAN路由器用於透過Cisco Umbrella DNS使用API金鑰/金鑰身份驗證方法進行註冊的數位證書已於2024年9月30日到期。證書過期的Cisco SD-WAN路由器將無法向Cisco Umbrella DNS服務註冊。此問題不適用於基於Token的Umbrella DNS註冊身份驗證。

有關詳細資訊，請參閱FN74166 中的思科Umbrella DNS證書於2024年9月30日到期。

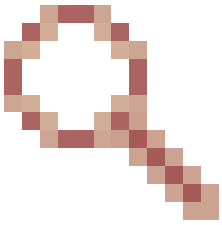
具有過期的umbrella根CA證書的受影響SD-WAN裝置無法與Cisco Umbrella DNS建立安全連線以進行裝置註冊。 由於裝置未向Umbrella DNS服務註冊，因此SD-WAN邊緣不會將終端使用者DNS請求重定向到Umbrella域伺服器以執行DNS安全策略。來自SD-WAN邊緣後方終端使用者的DNS請求不會被丟棄，並由終端使用者裝置上配置的DNS域伺服器提供服務。

瑕疵資訊

證書已更新為思科漏洞ID CSCwi43360



：DNS安全註冊到Umbrella雲的證書將於2024年9月到期。（在17.9.6、17.12.4、17.15.1a中修正）



即使證書正在更新，也無法建立SSL握手，這會在思科漏洞ID CSCwm中定址73365
：SSL握手失敗，儘管umbrella_root_ca.ca且裝置上存在最新的證書。（已於17.6.8a中修正）

固定已核發

CCO版本

版本	17.6.8安

修正矩陣

版本	思科建議的修正步驟
17.3.x/17.4.x/17.5.x	請遵循第1節中的步驟。在控制器模式下運行Cisco IOS XE軟體版本17.5.x或更早版本的思科裝置
17.6.1-17.6.7、17.7.x、17.8.x	請遵循第2部分中的步驟。在控制器模式下運行Cisco IOS XE軟體版本17.6.x到17.8.x的Cisco裝置
17.6.8安	Umbrella DNS證書到期問題已在此版本中修復。
17.9.1 – 17.9.4、17.10.x、17.11.x、17.12.1-17.12.2、17.13.x、17.14.x、17.15.1a	使用Umbrella DNS證書指令碼將證書自動複製到邊緣裝置。請參閱GIT上的Readme檔，以取得執行指令碼的步驟。
17.9.5安	請遵循第3節中的步驟
17.9.6	請遵循第4節中的步驟
17.12.3安	請遵循第5節中的步驟
17.12.4	請遵循第6節中的步驟

1. 在控制器模式下運行Cisco IOS XE軟體版本17.5.x或更早版本的思科裝置

使用補救選項安裝新的Umbrella RootCA證書。

自動

1. 對於SD-WAN Manager 20.9.1或更高版本，請使用Umbrella DNS證書指令碼從vManage自動

將證書複製到邊緣裝置。
2. Umbrela DNS證書指令碼
3. 請參閱GIT上的Readme檔，以取得使用指令集的詳細步驟。
4. 將RootCA證書複製到裝置後，重新載入路由器以完成安裝過程。

手動

1. 從New Umbrella Certificate網站下載新的未過期證書，然後將其放在能夠訪問SD-WAN重疊中受影響路由器的裝置上。
2. 輸入Linux scp命令或類似機制，從下載裝置向每個受影響的路由器執行安全檔案複製。

   舉例來說：

   scp ./isrgrootx1.pem <使用者名稱>@<EdgeIP>：trustidrootx3_ca.ca

   用管理員使用者替換<Username>，用受影響路由器的IP地址替換<EdgeIP>。

3. 將RootCA證書複製到裝置後，重新載入路由器以完成安裝過程。

2. 在控制器模式下運行Cisco IOS XE軟體版本17.6.x到17.8.x的Cisco裝置

使用補救選項安裝新的Umbrella RootCA證書。

自動

1. 對於SD-WAN Manager 20.9.1或更高版本，請使用Umbrella DNS證書指令碼從vManage自動將證書複製到邊緣裝置。
2. Umbrella DNS證書指令碼
3. 請參閱GIT上的Readme檔，以取得使用指令集的詳細步驟。
4. 將RootCA證書複製到裝置後，重新載入路由器以完成安裝過程。

手動

1. 從New Umbrella Certificate網站下載新的未過期證書，然後將其放在能夠訪問SD-WAN重疊中受影響路由器的裝置上。
2. 輸入Linux scp命令或類似機制，從下載裝置到每個受影響的路由器執行安全檔案複製。

   舉例來說：

   scp ./isrgrootx1.pem admin@<EdgeIP>：trustidrootx3_ca_092024.ca

   用受影響路由器的IP地址替換<EdgeIP>。

3. 將RootCA證書複製到裝置後，重新載入路由器以完成安裝過程

3. 在控制器模式下運行Cisco IOS XE軟體版本17.9.5a的思科裝置

使用補救選項來安裝新的Umbrella RootCA證書（如本節所述），對於大多數平台，存在可使用該

修復的HOT SMU。您還可以選擇運行提及的指令碼來安裝新的Umbrella RootCA證書。

1. HOT SMU適用於這些平台-「無中斷/建議的SMU，SSL握手失敗，儘管umbrella_root_ca.ca且裝置上存在最新證書」：

   4431整合式服務路由器
   4451-X整合式服務路由器

   ASR 1001-X路由器
   虛擬路由器
   4331整合式服務路由器
   4221整合式服務路由器
   4351整合式服務路由器
   Catalyst 8500L邊緣平台
   ASR 1001-HX路由器
   4321整合式服務路由器

   Catalyst 8500邊緣平台

   4461整合式服務路由器

2. 或者，也可以使用SMU運行指令碼Umbrella DNS證書指令碼請參閱GIT上的Readme檔案，瞭解使用該指令碼的詳細步驟。

僅指令碼選項：
ASR1002-X路由器

Catalyst 8300邊緣平台

運行Cisco IOS XE SD-WAN的ISR 1000系列

4. 在控制器模式下運行Cisco IOS XE軟體版本17.9.6的Cisco裝置

1. HOT SMU適用於這些平台-「無中斷/建議的SMU，SSL握手失敗，儘管umbrella_root_ca.ca且裝置上存在最新證書」：

   4221整合式服務路由器
   4321整合式服務路由器
   4451-X整合式服務路由器
   Catalyst 8500邊緣平台
   4431整合式服務路由器
   虛擬路由器
   4461整合式服務路由器
   4331整合式服務路由器
   4351整合式服務路由器
   ASR 1001-HX路由器
   ASR 1001-X路由器
   Catalyst 8500L邊緣平台

3. 或者，也可以使用SMU運行指令碼Umbrella DNS證書指令碼請參閱GIT上的Readme檔案，瞭解使用該指令碼的詳細步驟。

僅指令碼選項：

ASR1002-X路由器

Catalyst 8300邊緣平台

運行Cisco IOS XE SD-WAN的ISR 1000系列

5. 在控制器模式下為Cisco IOS XE軟體版本17.12.3a的思科裝置

1. HOT SMU適用於這些平台-「無中斷/建議的SMU，SSL握手失敗，儘管umbrella_root_ca.ca且裝置上存在最新證書」：

   4221整合式服務路由器
   Catalyst 8300邊緣平台
   4331整合式服務路由器
   4461整合式服務路由器
   1100整合式服務路由器
   4351整合式服務路由器
   4321整合式服務路由器
   4431整合式服務路由器
   虛擬路由器
   4451-X整合式服務路由器

   Catalyst 8500L邊緣平台
   Catalyst 8500邊緣平台
   ASR 1001-HX路由器

2. 替代SMU，運行指令碼Umbrella DNS證書指令碼

請參閱GIT上的Readme檔，以取得使用指令集的詳細步驟。

6. 在控制器模式下運行Cisco IOS XE軟體版本17.12.4的思科裝置

1. HOT SMU適用於這些平台-「無中斷/建議的SMU，SSL握手失敗，儘管umbrella_root_ca.ca且裝置上存在最新證書」：

   Catalyst 8500邊緣平台
   ASR 1001-HX路由器
   4331整合式服務路由器
   4321整合式服務路由器
   4221整合式服務路由器
   虛擬路由器
   4351整合式服務路由器

4451-X整合式服務路由器
4461整合式服務路由器
Catalyst 8300邊緣平台
ASR 1002-HX路由器
4431整合式服務路由器

1100整合式服務路由器

Catalyst 8500L邊緣平台

2. 或者，您也可以使用SMU來運行指令碼Umbrella DNS證書指令碼。請參閱GIT上的Readme檔案，瞭解使用該指令碼的詳細步驟。

⚠ 注意：只要不重新啟動裝置或者沒有新註冊，來自裝置的Umbrella DNS註冊將繼續運行。

⚠ 注意：如果刪除並重新應用umbrella配置，則會觸發重新註冊umbrella DNS。只要不遵循此過程，UMBRELLA DNS就會正常運行。

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）。