

解決標籤Umbrella根CA的安全工具

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[NIST建議](#)

[其他資訊](#)

簡介

本文說明安全稽核工具將Umbrella Root CA數位證書標籤為風險的原因。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella安全Web闡道(SWG)。

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。

概觀

用於掃描Umbrella基礎架構的某些安全稽核工具可以報告Cisco Umbrella Root CA數位證書具有2048位RSA金鑰，並且在2030年之後過期。根據工具和組織的安全策略，可以將金鑰大小和/或到期日期標籤為可能需要補救的風險。檢視本文中的資訊，確定您的組織是否需要接受審計工具的建議。

NIST建議

數位證書金鑰長度隨時間變化的建議（包括2030日期的2048位RSA金鑰）由美國國家標準研究院(NIST)發佈。包含這些建議的文檔是SP 800-57第1部分修訂版5:金鑰管理建議。

「表4，安全強度時間幀」（第59頁）指出，相當於112個對稱金鑰位的安全強度在2030年後對「傳統使用」有效（RSA 2048位非對稱金鑰相當於大約116位對稱金鑰強度）。使用現有根證書（例如

Cisco Umbrella根CA證書) 屬於此類別，因此這被視為合規使用。在2030年之後簽髮帶有2048位金鑰的證書不符合建議。

其他著名的公共證書頒發機構繼續使用具有2048位RSA金鑰和2030年到期日期的根證書。檢視DigiCert文檔：例如，由DigiCert頒發的Global Root CA證書和Assured ID Root CA證書等DigiCert Trusted Root Authority證書。

遠在2030年之前，Cisco Umbrella可以頒發一個或多個符合NIST建議且金鑰大小較大的新根證書。

其他資訊

組織可以自由決定NIST建議是否滿足其需求。如果您對此問題有進一步的擔憂，思科有一個專門的PKI團隊，負責監督思科的受信任根儲存和PKI合規性計畫。Cisco PKI團隊提供的其他資訊(包括思科頒發的所有公共證書、證書策略和實踐宣告以及其他文檔)可在[Cisco PKI中獲得:策略、證書和文檔](#)。如有其他問題，可通過電郵傳送至PKI團隊：ciscopki-public@external.cisco.com。

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）。