

瞭解Umbrella中的公鑰固定和憑證固定功能

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[與Umbrella SWG的相容性](#)

[其他證書固定應用程式](#)

簡介

本檔案介紹在Cisco Umbrella中的憑證固定和公共金鑰固定。

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。

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

證書固定是一種網際網路安全機制，它允許應用程式抵制使用錯誤頒發或欺詐性數位證書對HTTPS伺服器進行模擬。它通過將伺服器與一組已定義的公鑰關聯來做到這一點，這些公鑰可能是與該伺服器連線的唯一受信任公鑰。證書固定有兩種技術：

- 公鑰固定(PKP RFC7469)是一種現在過時的機制，用於在Web瀏覽器中觸發憑證固定。固定的證書將使用HTTP標頭傳送到瀏覽器。
- 靜態憑證固定是指應用程式採用硬式編碼，以便預期特定憑證或憑證授權單位。某些案頭/移動應用使用靜態證書固定機制來提高安全性。

當這些Web應用程式由Umbrella代理時，Umbrella提供的公鑰不匹配，從而導致應用程式關閉HTTPS連線。證書固定通常只適用於案頭/移動應用程式，因為現代Web瀏覽器已刪除PKP支援。

與Umbrella SWG的相容性

Umbrella會繞過來自SSL解密的已知URL，以便在某些情況下解決證書固定問題。表1包括所有Umbrella客戶已全域性繞過的應用程式。表1還包括在當時或寫入時已知使用證書定位的其他應用程式。如果您使用的是這些應用程式中的任意一個，則可以考慮使用後面介紹的方法（出於給出的原因）從HTTPS檢查中繞過應用程式。表2提供了表1中涵蓋的應用程式服務的更多詳細資訊。

其他證書固定應用程式

使用Umbrella的[Selective](#) Decryption功能，可以針對每個客戶（每個策略）繞過應用程式，以解決證書固定問題。這些例外可以根據域、應用程式名稱或類別輕鬆實施；Umbrella SWG在我們的應用程式資料庫中包含大量的應用程式。

在大多數情況下，是否繞過應用程式由IT管理員決定。新增解密例外是一種安全權衡，因為它阻止對Web內容進行安全/檔案檢查。這是一個單獨的決策，取決於應用程式型別和業務需求。例如，如果證書固定問題僅影響移動/案頭應用程式，管理員可以選擇新增例外來使移動應用程式工作，或者更願意讓使用者使用該應用程式的Web版本。

這是一個應用表，這些應用對於Umbrella客戶被全域性繞過，且在編寫時不需要或已知使用證書固定操作，並且在預設情況下不被Umbrella繞過。如果您使用的是預設情況下不會繞過的應用程式，則可以考慮使用上述方法（出於給出的原因）從HTTPS檢查中繞開應用程式。

表1 — 可以使用證書固定的應用程式

應用程式名稱	思科資安防護傘
Adobe服務	Umbrella客戶在全球範圍內繞過
Airbnb	受Application Control支援
亞馬遜Alexa	受Application Control支援
Amazon Drive	受Application Control支援
亞馬遜Kindle	受Application Control支援
Amazon Workspaces	受Application Control支援
振幅	Umbrella客戶在全球範圍內繞過

應用動態	Umbrella客戶在全球範圍內繞過
Apple iMessage	受Application Control支援
Apple Mail	受Application Control支援
Apple服務(有關更多詳細資訊，見表2)	Umbrella客戶在全球範圍內繞過
思科服務(請參閱表2瞭解詳情)	Umbrella客戶在全球範圍內繞過
Citrix Workspace	受Application Control支援
克拉什萊蒂克	Umbrella客戶在全球範圍內繞過
CrowdStrike獵鷹	受Application Control支援
Diligent.com	受Application Control支援
不和諧聊天	Umbrella客戶在全球範圍內繞過
DocuSign雲端協定	受Application Control支援
DropBox	受Application Control支援
Druva雲備份	受Application Control支援
Egyte Connect	受Application Control支援
Evernote	受Application Control支援
Facebook Messenger	受Application Control支援
臉書	受Application Control支援
檔案電子郵件	受Application Control支援

四方	受Application Control支援
Giphy	Umbrella客戶在全球範圍內繞過
GitHub	受Application Control支援
Google Drive	受Application Control支援
Google Play商店	受Application Control支援
Google服務(有關更多詳細資訊，見表2)	Umbrella客戶在全球範圍內繞過
Google工作空間	受Application Control支援
GoToMeeting	受Application Control支援
炒作機	受Application Control支援
Instagram	受Application Control支援
LogMein Pro	受Application Control支援
Microsoft Defender for Endpoint	受Application Control支援
Microsoft Intune	受Application Control支援
Microsoft服務(請參閱表2瞭解詳細資訊)	Umbrella客戶在全球範圍內繞過
Microsoft Xbox Live	受Application Control支援
Netflix	受Application Control支援
OpenDrive	受Application Control支援
PayPal	受Application Control支援

PingOne身份	受Application Control支援
Rackspace/雲端驅動器服務	Umbrella客戶在全球範圍內繞過
Salesforce CRM	受Application Control支援
網段	Umbrella客戶在全球範圍內繞過
訊號平台	受Application Control支援
Skype for Business	受Application Control支援
Snapchat	受Application Control支援
Soundcloud	受Application Control支援
蜘蛛橡樹	受Application Control支援
Spotify	受Application Control支援
TeamViewer	受Application Control支援
抖音	受Application Control支援
托多斯特	受Application Control支援
推特	受Application Control支援
維密歐	受Application Control支援
工作日HCM	受Application Control支援
縮放會議	Umbrella客戶在全球範圍內繞過

表2 -詳細資訊如表1所示的全域性繞過的服務

Apple服務	• Apple強制網路門戶檢查 • Apple iTunes和App Store • 其他蘋果平台服務
思科服務	• Cisco Umbrella和OpenDNS服務 • 思科Webex和Webex Teams • Cisco Cloud Email Security WebUI • AMP終端服務 • Duo Security 2FA
Google服務	• Google環路 • Web上的Google消息 • 其他Google平台服務
Microsoft服務	• Microsoft網路連線狀態指示器 • Windows更新 • Windows翻譯服務 • 其他Microsoft/Windows平台服務

有關其他幫助，請參閱對非瀏覽器應用程式進行故障排除或與[Umbrella支援部門](#)聯繫。在工程團隊稽核這些應用後，可以考慮將其新增到我們的全域性旁路清單中。

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）。