Google驅動器安全下載期間的CRYPTO_INTERNAL_ERROR

目錄

問題

加密的Google Sheets檔案在通過啟用流量解密的Cisco Secure Access訪問時無法開啟。使用者在Google Drive安全下載期間會遇到CRYPTO_INTERNAL_ERROR。當安全Web網關(SWG)檢查處於活動狀態時，會發生此問題，因為在解密和檢查過程中忽略Range報頭，從而導致干擾Google安全下載機制。

此問題會影響使用RAVPN+ZTA實施的環境，並影響對大量使用者訪問加密的Google Sheets。

環境

- 技術：思科安全存取（解決方案支援）
- 子技術：安全訪問
- 實現：RAVPN+ZTA（遠端訪問VPN +零信任訪問）
- 受影響的元件：ZTA配置檔案
- 受影響的域：clients6.google.com和其他與Google Drive相關的域

解析

解決方案涉及實施臨時解決方法，同時監控永久供應商端修復。

在接下來的章節中概述的方法已經過驗證，可以恢復對加密的Google表格的訪問。

臨時解決方法選項

選項 1:禁用流量解密

完全禁用受影響使用者組或策略的流量解密。這將恢復Google Sheets訪問，但會刪除所有基於解密的安全檢查功能。

選項 2:從解密中排除Google驅動器域

將與Google驅動器相關的域新增到安全訪問策略配置中的不解密清單：

- clients6.google.com
- 流量分析中確定的其他與Google Drive相關的域

此方法可以維護其他流量的解密，同時允許Google工作表正常運行。但是，此解決方法可以權衡禁用排除域的CASB Google驅動器上傳阻止功能。

技術分析與監控

思科分析確認，安全Web網關檢查會忽略Range標頭，以實現檔案內容的全面安全掃描。此行為會干擾Google Drive安全下載過程，該過程依賴範圍標頭來獲得正確的解密流。

Google已承認此問題，並確認代理行為（包括Cisco Umbrella/network proxy）通過刪除或重寫範圍標頭來干擾Google Drive安全下載請求。這會強制下載完整檔案，從而破壞Google解密機制。谷歌正在開發客戶端解決方案，不過尚未提供預計到達時間。

實施注意事項

實施變通方法的組織應考慮安全影響：

- 評估從解密檢查中排除Google Drive域的風險。
- 檢查可能受域排除影響的CASB策略。
- 記錄將來政策審查的臨時變通方法。
- 監視Google提供的有關客戶端修復程式開發的更新。

原因

根本原因是思科安全訪問SWG檢查行為與Google Drive安全下載機制之間的相容性問題。

具體為：

在解密和安全掃描過程中，Cisco安全Web網關檢查會忽略Range標頭，以確保完成檔案分析。但是，Google Drive加密檔案訪問依賴於Range標頭來正確處理用於安全下載的解密流。在代理檢查過程中刪除或修改這些報頭時，Google客戶端解密失敗，導致CRYPTO_INTERNAL_ERROR。

這表示安全檢查要求（完整檔案掃描）和Google加密檔案傳送機制（基於範圍的安全下載）之間存在根本的不相容性。

相關內容

- 思科技術支援與下載

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）。