本文件為以下英文版內容譯文 https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/。此譯本僅供參考和方便之用。如有任何衝突或歧義，應一律以英文版為準。

執行摘要

CrowdStrike 初步事後審查 (PIR)：影響 Falcon 感測器和 Windows 作業系統的內容設定更新 (BSOD)

概述

為防患未然以因應新型且不斷演化的網路威脅，安全產品會定期提供內容更新。此類更新可包括收集遙測資料、新威脅偵測模式、漏洞偵測和其他重要改善。藉由定期更新，安全產品可以快速因應新興威脅，確保為使用者及其系統提供強大的防護。

經過：事件概況

世界標準時間 2024 年 7 月 19 日 04:09，Falcon 感測器的快速回應內容更新已發布至運行 7.11 及更高版本感測器的 Windows 主機。此更新旨在收集有關 CrowdStrike 觀察到之新威脅技術的遙測資料，但在世界標準時間 04:09 至 05:27 之間導致線上系統當機 (BSOD)。Mac 和 Linux 主機未受影響。在此期間未上線或未連線的 Windows 主機不受影響。

原委：事發原因

當機由快速回應內容中的缺陷引起，驗證檢查期間並未發現該缺陷。Falcon 感測器載入內容時，該缺陷導致記憶體讀取越界，進而致使 Windows 當機 (BSOD)。

CrowdStrike 正在採取哪些措施來防範此種情況再次發生？

增強軟體測試程序

- 透過使用本機開發人員、內容更新和回溯測試、壓力測試、模糊測試、故障注入、穩定性和內容介面測試等測試類型來改良快速回應內容測試。
- 在內容驗證器中引進額外的驗證檢查，以免類似問題再次出現。

增強韌性與復原能力

- 加強 Falcon 感測器中的錯誤處理機制，確保妥善管理有問題內容所導致的錯誤。

精細的部署策略

- 採用分階段部署策略，先對一小部分系統進行金絲雀部署(canary deployment)，然後再進一步實施分階段部署。
- 在分階段內容部署期間加強對感測器和系統效能的監控，以立即識別並緩解問題。
- 允許對部署此類更新的時間和位置進行細化選擇，進而為客戶提供對快速回應內容更新交付的更大掌控度。
- 提供內容更新與時間安排的通知。

第三方驗證

- 進行多重獨立第三方安全程式代碼審查。
- 從開發到部署，進行端對端品質流程獨立審查。