本文書は、https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.掲載のインシデント事後のプレレビュー（PIR）のExecutive Summaryの英語版の翻訳です。本翻訳版は、参照を容易にし、便宜上の目的でのみ提供されています。矛盾や曖昧さが生じた場合は、常に英語版が優先されます。

エグゼクティブサマリー

クラウドストライクのインシデント事後のプレレビュー（PIR）：Falcon センサーと Windows オペレーティングシステム（BSOD）に影響を及ぼしたコンテンツコンフィグレーションの更新について

概要

新たに進化するサイバー脅威をいち早く捉えるため、セキュリティ製品では定期的にコンテンツのアップデートを提供しています。これらのアップデートには、テレメトリ収集、新しい脅威検知パターン、脆弱性の検知、その他の重要な改善などが含まれます。定期的にアップデートを行うことで、セキュリティ製品は新たな脅威に迅速に対応し、当社の製品をご利用のお客様とそのシステムを確実に保護することができます。

発生事象の概要

2024年7月19日04:09（UTC時間）、Falcon センサーのラピッドレスポンスコンテンツに関するアップデートが、センサーバージョン7.11以上を実行している Windows ホストを対象に公開されました。このアップデートは、クラウドストライクが観察した新たな脅威手法に関するテレメトリを収集するためのものでしたが、04:09から05:27（UTC時間）にオンラインだったシステムがクラッシュ（BSOD）するという結果を引き起こしました。Mac ホストと Linux ホストは影響を受けませんでした。この期間にオフライン、または接続しなかった Windows ホストは影響を受けませんでした。

発生事象の原因

このクラッシュは、ラピッドレスポンスコンテンツの欠陥によるもので、検証チェックでは検出されませんでした。Falcon センサーによってコンテンツが読み込まれた際、境界外メモリを読み出し、Windows のシステムがクラッシュ（BSOD）するという結果を引き起こしました。

クラウドストライクの再発防止策について

ソフトウェアテスト手順の強化

- ラピッドレスポンスコンテンツテストを、次のテストタイプを使用することにより改善します。ローカルデベロッパーテスト、コンテンツの更新およびロールバックテスト、ストレステスト、ファジング、フォールトインジェクション、安定性テスト、コンテンツインターフェーステストです。
- 同様の問題を防ぐため、コンテンツバリデーターにさらにバリデーションチェックを導入します。

回復力と復元力の強化

- Falcon センサーのエラー処理メカニズムを強化し、問題のあるコンテンツのエラーが適切に管理されるようにします。

展開戦略の改良

- 時差展開戦略を実施し、システムのごく一部を対象とするカナリア展開から始め、その後さらに段階的なロールアウトを展開します。
- コンテンツを時差展開している間、問題を迅速に特定して緩和できるよう、センサーとシステムのパフォーマンスの監視を強化します。
- ラピッドレスポンスコンテンツの更新日時と具体的な展開先をお客様が細かく選択できるようにし、更新の配布に関する制御方法の精度を上げて提供します。
- コンテンツ更新やタイミングをお知らせします。

第三者機関による検証

- 独立した第三者によるセキュリティコードレビューを複数回実施します。
- 開発から展開までのエンドツーエンドの品質プロセスについて、独立したレビューを実施します。