Dieses Dokument ist eine Übersetzung der folgenden englischen Version https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. Diese übersetzte Version dient ausschließlich der einfacheren Bezugnahme und Zweckmäßigkeit. Im Falle von Widersprüchen oder einer Unklarheit hat die englische Version stets Vorrang.

Executive Summary

Preliminary Post Incident Review (PIR): Content Konfigurationsupdate mit Auswirkungen auf den Falcon-Sensor und das Windows-Betriebssystem (BSOD)

Überblick

Um neuen und sich kontinuierlich entwickelnden Cyberbedrohungen immer einen Schritt voraus zu sein, liefern Sicherheitsprodukte routinemäßig Content Updates. Zu diesen Updates gehören das Erfassen von Telemetriedaten, neue Bedrohungserkennungsmuster, die Erkennung von Schwachstellen und andere entscheidende Verbesserungen. Durch regelmäßige Updates können sich Sicherheitsprodukte schnell an aufkommende Bedrohungen anpassen und so einen robusten Schutz für Benutzer und ihre Systeme gewährleisten.

Was passiert ist: Überblick über den Vorfall

Am 19. Juli 2024 um 04:09 Uhr UTC wurde ein Rapid Response Content Update für den Falcon-Sensor an Windows-Hosts mit der Sensor Version 7.11 und höher bereitgestellt. Diese Aktualisierung sollte Telemetriedaten über neue Bedrohungstechniken, die von CrowdStrike beobachtet wurden, erfassen. Sie führte zu Abstürzen (BSOD) auf Systemen, die zwischen 04:09 und 05:27 Uhr UTC online waren. Mac- und Linux-Hosts waren nicht betroffen. Windows-Hosts, die in diesem Zeitraum nicht online waren oder keine Verbindung hatten, waren nicht betroffen.

Warum es passiert ist: Ursache des Vorfalls

Die Abstürze waren auf einen Fehler im Rapid Response Content zurückzuführen, der bei der Validierung unentdeckt blieb. Das Laden des Inhalts durch den Falcon-Sensor verursachte einen unzulässigen Speicherzugriff, der zu Windows-Abstürzen (BSOD) führte.

Was unternimmt CrowdStrike, um zu verhindern, dass so etwas noch einmal passiert?

Erweiterte Software-Testverfahren

- Optimierung der Tests des Rapid Response Content durch Nutzung von Testtypen wie z. B.: lokale Tests durch Entwickler, Content Update und Rollback, Stresstests, Fuzzing, Fault Injection, Stabilitätstests und Testen von Content-Schnittstellen.
- Einführung zusätzlicher Validierungsprüfungen zum Content-Validator, um ähnliche Probleme zu vermeiden.

Verbesserte Resilienz und Wiederherstellbarkeit

- Stärkung der Mechanismen zur Fehlerbehandlung im Falcon-Sensor, um sicherzustellen, dass Fehler durch problematischen Content auf anwenderfreundliche Art und Weise verarbeitet werden.

Neu definierte Bereitstellungsstrategie

- Einführung einer gestaffelten Bereitstellungsstrategie, beginnend mit einer Canary-Releasebereitstellung auf einer kleinen Untergruppe von Systemen, bevor ein weiterer schrittweiser Rollout erfolgt.
- Verbesserung der Überwachung von Sensor- und Systemleistung während der gestaffelten Bereitstellung von Content, um Probleme umgehend zu erkennen und zu beheben.

- Mehr Kontrolle unserer Kunden über die Bereitstellung von Rapid Response Content Updates, indem eine granularere Auswahl, wann und wo diese Updates bereitgestellt werden, ermöglicht wird.
- Benachrichtigungen über Content Updates und Timing.

Validierung durch Dritte

- Durchführung mehrerer unabhängiger Sicherheitsüberprüfungen des Programmcodes durch Dritte.
- Durchführung unabhängiger Überprüfungen des gesamten Qualitätsprozesses, von der Entwicklung bis zur Bereitstellung.