EXECUTIVE SUMMARY

CrowdStrike Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)

Overview

To stay ahead of new and evolving cyber threats, security products routinely deliver content updates. These updates can include gathering telemetry, new threat detection patterns, vulnerability detections, and other crucial improvements. By regularly updating, security products can quickly adapt to emerging threats, ensuring robust protection for users and their systems.

What Happened: Incident Overview

On July 19, 2024, at 04:09 UTC, a Rapid Response Content update for the Falcon sensor was published to Windows hosts running sensor version 7.11 and above. This update was to gather telemetry on new threat techniques observed by CrowdStrike, but triggered crashes (BSOD) on systems that were online between 04:09 and 05:27 UTC. Mac and Linux hosts were not impacted. Windows hosts that were not online, or did not connect during this period, were not impacted.

Why It Happened: Cause of Incident

The crashes were due to a defect in the Rapid Response Content, which went undetected during validation checks. When the content was loaded by the Falcon sensor, this caused an out-of-bounds memory read, leading to Windows crashes (BSOD).

What is CrowdStrike Doing to Prevent This From Happening Again?

Enhanced Software Testing Procedures

- Improve Rapid Response Content testing by using testing types such as: local developer, content update and rollback, stress, fuzzing, fault injection, stability, and content interface testing.
- Introduce additional validation checks in the Content Validator to prevent similar issues.

Enhanced Resilience and Recoverability

- Strengthen error handling mechanisms in the Falcon sensor to ensure errors from problematic content are managed gracefully.

Refined Deployment Strategy

- Adopt a staggered deployment strategy, starting with a canary deployment to a small subset of systems before a further staged rollout.
- Enhance monitoring of sensor and system performance during the staggered content deployment to identify and mitigate issues promptly.
- Provide customers with greater control over the delivery of Rapid Response Content updates by allowing granular selection of when and where these updates are deployed.
- Provide notifications of content updates and timing.

Third Party Validation

- Conduct multiple independent third-party security code reviews.
- Conduct independent reviews of end-to-end quality processes from development through deployment.