# Executive Summary: Root Cause Analysis — Channel File 291

***This document provides an executive summary of the findings of CrowdStrike's Root Cause Analysis (RCA) report. The full report elaborates on the information previously shared in our preliminary Post Incident Review (PIR), providing further depth on the findings, mitigations, technical details and root cause analysis of the incident.***

## *Introduction*

CrowdStrike was founded with a mission to protect customers against today's adversaries and stop breaches. On July 19, 2024, as part of regular operations, CrowdStrike released a content configuration update (via channel files) for the Windows sensor that resulted in a system crash. We apologize unreservedly.

We acknowledge the incredible round-the-clock efforts of our customers and partners who, working alongside our teams, mobilized immediately to restore systems and bring many back online within hours. As of July 29, 2024, at 8:00 p.m. EDT, ~99% of Windows sensors were online, compared to before the content update. We typically see a variance of ~1% week-over-week in sensor connections. To any customers still affected, please know we will not rest until all systems are restored.

## *What Happened*

The CrowdStrike Falcon sensor delivers AI and machine learning to protect customer systems by identifying and remediating the latest advanced threats. In February 2024, CrowdStrike introduced a new sensor capability to enable visibility into possible novel attack techniques that may abuse certain Windows mechanisms. This capability pre-defined a set of fields for Rapid Response Content to gather data. As outlined in the RCA, this new sensor capability was developed and tested according to our standard software development processes.

On March 5, 2024, following a successful stress test, the first Rapid Response Content for Channel File 291 was released to production as part of a content configuration update, with three additional Rapid Response updates deployed between April 8, 2024 and April 24, 2024. These performed as expected in production.

On July 19, 2024, a Rapid Response Content update was delivered to certain Windows hosts, evolving the new capability first released in February 2024. The sensor expected 20 input fields, while the update provided 21 input fields. In this instance, the mismatch resulted in an out-of-bounds memory read, causing a system crash. Our analysis, together with a third-party review, confirmed this bug is not exploitable by a threat actor.

While this scenario with Channel File 291 is now incapable of recurring, it informs the process improvements and mitigation steps that CrowdStrike is deploying to ensure further enhanced resilience.

## *What We Did and What's Next*

Based on the findings in the RCA, here are some of the actions CrowdStrike has taken and will take moving forward:

- **Update Content Configuration System test procedures.** This work has been completed. This includes upgraded tests for Template Type development, with automated tests for all existing Template Types. Template Types are part of the sensor and contain predefined fields for threat detection engineers to leverage in Rapid Response Content.

- **Add additional deployment layers and acceptance checks for the Content Configuration System.** This work has been completed with an updated deployment ring process, ensuring Template Instances pass successive deployment rings before rollout into production.

- **Provide customers additional control over the deployment of Rapid Response Content updates.** New capabilities have been implemented and deployed to our cloud that allow customers to control how Rapid Response Content is deployed, with additional functionality planned for the future.

- **Prevent the creation of problematic Channel 291 files**. Validation for the number of input fields has been implemented to prevent this issue from happening.

- **Implement additional checks in the Content Validator.** Additional checks are planned for release into production by August 19, 2024.

- **Enhance bounds checking in the Content Interpreter for Rapid Response Content in Channel File 291.** Bounds checking was added on July 25, 2024, with general availability expected August 9, 2024. These fixes are being backported to all Windows sensor versions 7.11 and above through a sensor software hotfix release.

- **Engage two independent third-party software security vendors to conduct further review of the Falcon sensor code and end-to-end quality control and release processes**. This work has begun and will be ongoing as part of our focus on security and resilience by design.

For additional details and defined terms, please refer to the RCA.