Crowdstrike's Update Failure Root Cause Analysis: Executive Summary

What Happened

On July 19th 2024, as part of their regular release operations, Crowdstrike released a content configuration update for the windows sensor that resulted in a system crush (BSOD).

The **Crowdstrike Falcon Sensor** utilizes AI and Machine Learning to protect customer systems by automatically detecting and remediating latest advanced threats. These models are kept up-to-date and strengthened with learnings from the latest threat telemetry from the sensor and human intelligence from Falcon Adversary OverWatch, Falcon Complete and CrowdStrike threat detection engineers.

On February 2024, Crowdstrike introduced a new sensor capability to enable visibility into possible novel techniques that may abuse certain Windows processes. This capability predefined a set of fields for **Rapid Response Content** (later explained in the extract) to gather data. This new capability was developed, tested and passed Crowdstrike's standard software development processes.

On July 19th 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, whereas the update provided 21 input fields. This mismatch resulted in an *out-of-bounds memory read*, causing the system crush. This bug however is not exploitable by a threat actor.

Systems in scope of this update; that were affected, include Windows hosts running Falcon sensor version 7.11 and above that were online between Friday, July 19, 2024 04:09 UTC and Friday, July 19, 2024 05:27 UTC and received the update. Mac and Linux hosts were not affected.

Rapid Response Content Explained

Crowdstrike's security model is built on stopping evolving cyber threats which requires effective threat intelligence and real-time information about IT infrastructures augmented by the experience of tens of thousands of enterprises. This and the speed of threat identification and response is what underlies their real-time detection and response security model.

Rapid Response Content (a mapping feature template) fine-tunes and enhances Crowdstrike's Falcon sensor's ability to observe specific behaviors at operational speed – without requiring changes on the sensor code. Rapid Response Content is delivered as "Template Instances" which map to specific behaviors for the sensor to observe, detect or prevent. Template Instances have a set of fields that are configured to match a desired behavior. It is the mismatch in these fields (between the Rapid Response Content Template and Sensor) that caused the crush.

Steps Taken by Crowdstrike to Prevent such an occurrence in the Future:

Software Resiliency and Testing

- Improve Rapid Response Content testing by using testing types such as:
  - Local developer testing
  - Content update and rollback testing
  - Stress testing, fuzzing and fault injection
  - Stability testing
  - Content interface testing
- Add additional validation checks/steps to the Content Validation for Rapid Response Content
- Enhance existing error handling in the Content Interpreter.

Crowdstrike also stated that its kernel driver, which is loaded early in the system boot process, enables the Falcon sensor to detect and defend against malware that launches before user-mode processes start.

The company plans to update their agent to leverage new support for security functions in user space, reducing dependency on the kernel driver.

Lessons Learned from Crowdstrike occurrence:

1. **Manual Fix Challenges:**

   a. Recovery is hard, time and money consuming as it is manual job.

   b. Recovery is slow without backups for all Virtual Desktop Infrastructures (VDIs).

   c. Encryption Key management: Recovery key is needed to access Safe Mode if Bitlocker (or other drive encryption) is enabled.

2. **Redundancy and Backup Plans:**
    a. Regular backups are essential for quick recovery
    b. Maintain robust backup systems and have alternative operational plans in place.
3. **Test Updates:**
    a. Updates must be tested in a controlled environment before wide deployment.
    b. No auto updates / auto upgrades trust
4. **Change Control:** Implement strict change control processes with rollback plans for any critical system changes.
5. **Vendor Management:** Build strong relationships with vendors and ensure they have solid incident response mechanisms.
6. **(Critical) 3rd Party Providers Management**: Frequent 3rd party providers and MSSPs assessment.
7. **Communication Strategy:** Develop a clear communication plan for stakeholders during incidents.
8. **Continuous Improvement:** Regularly review and update cybersecurity policies and procedures based on lessons learned from incidents.

Conclusion

In conclusion, the July 19th, 2024, incident involving CrowdStrike's Windows sensor update highlights critical areas for improvement in software resiliency and testing. The out-of-bounds memory read caused by a mismatch in input fields underscored the need for rigorous pre-deployment testing, robust backup systems, and stringent change control processes.

Development companies (and companies in general) are advised to improve error handling, while also reducing reliance on kernel drivers to bolster security. This incident serves as a crucial reminder of the importance of manual recovery planning, effective vendor management and continuous improvement in cybersecurity practices.

While this specific scenario is now incapable of recurring, it informs for process improvements and mitigation steps that CrowdStrike and other companies are deploying to ensure further enhanced resilience.

References:

More detailed Root Cause Analysis and research of the incident can be found from the links below;

https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/?s=09

https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

Information Sharing

We encourage any organization or individual that has any information related to this incident to share it with us through our email info@serianu.com or landline; +254 771949475 to allow us to further analyze and detect future potential threats.