



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

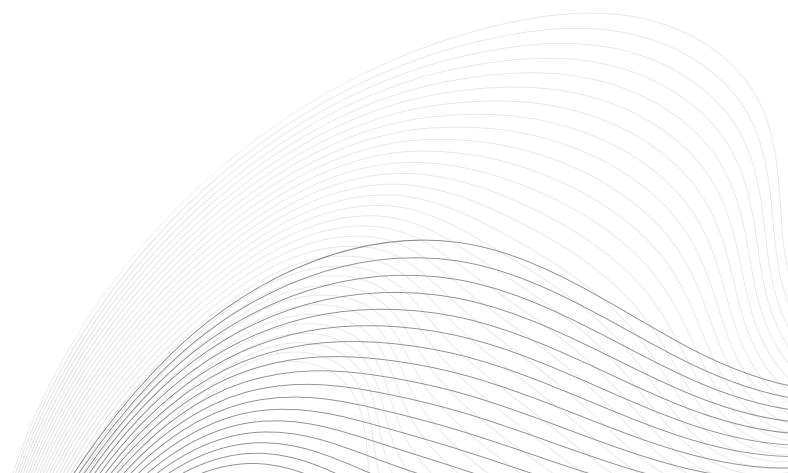
Advisory on CrowdStrike Falcon Sensor Incident and Vulnerability

July 2024



TABLE OF CONTENTS

Overview	03
Impact of IT Disruptions	04
Our Recommendation	05
Conclusion	06



Overview

On July 19, 2024, an update to the CrowdStrike Falcon sensor caused significant disruptions for Windows users globally. The update led to systems experiencing repeated blue screen of death (BSOD) errors with the message "DRIVER_OVERRAN_STACK_BUFFER," making them inoperable. This glitch affected Windows 10 and 11 systems running CrowdStrike's endpoint security software, particularly impacting enterprise customers, in the process thousands of devices globally, including critical production servers. CrowdStrike has acknowledged the problem and is actively working to resolve the same, advising users to follow their official communication channels for necessary updates and the required recovery procedures. This incident underscores the risks associated with automatic updates for security software and highlights the need for rigorous testing and staged rollout policies.

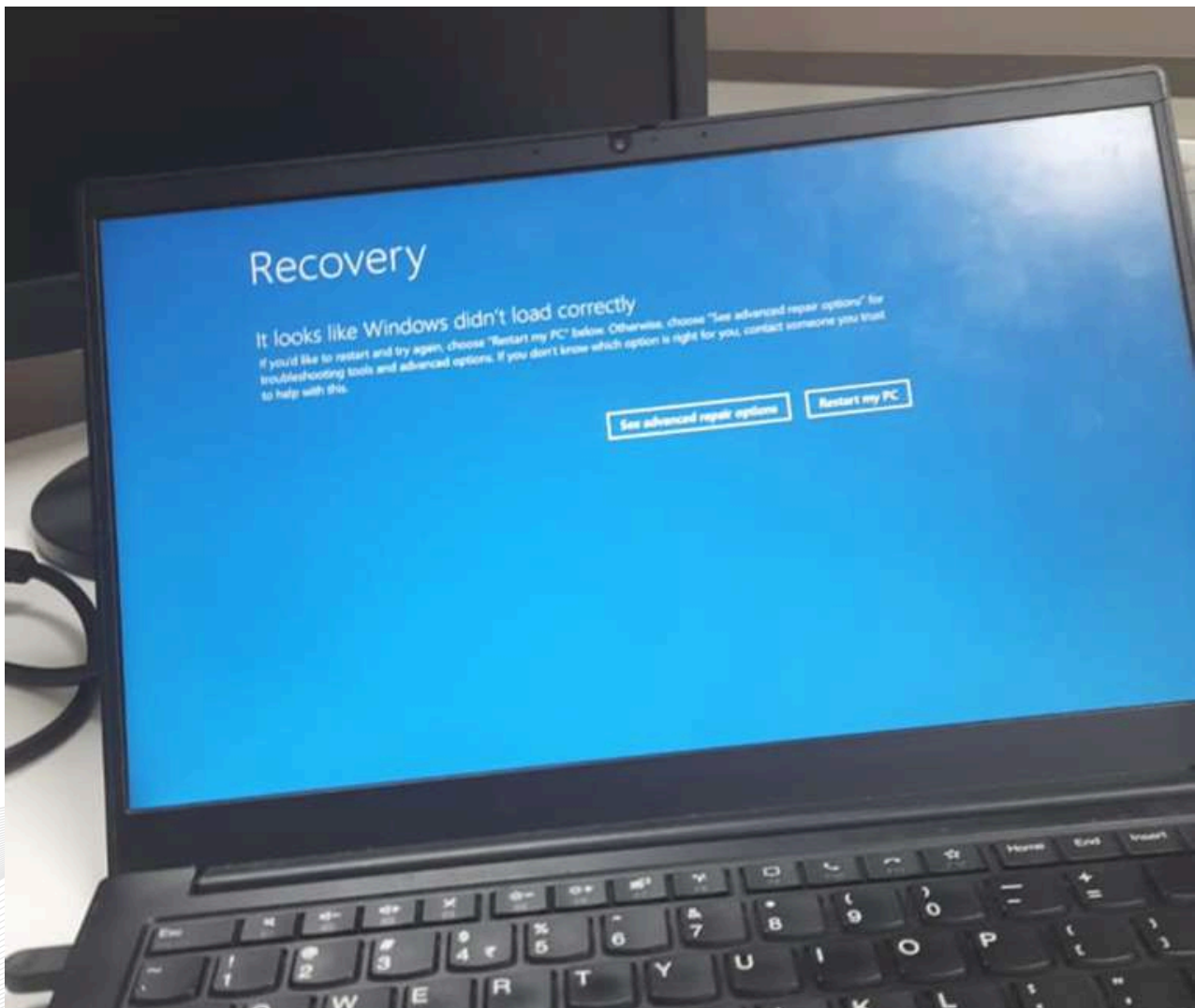


Fig: Affected Windows System

Impact of IT Disruptions

The disruption affected a wide range of services across multiple countries:

- Australia: Media, airlines, supermarkets, banks, and hospitals.
- Belgium: Train ticket sales, media, banks, airports, and government services.
- Canada: Banking apps and airports.
- China: Businesses allowed early dismissal due to blue screens.
- Croatia: Health information system and air traffic control issues.
- Czech Republic: Prague Airport affected.
- France: TV channels and Paris Olympics systems.
- Germany: Airports and hospitals.
- Hungary: Budapest Airport issues.
- Hong Kong: Airport check-in delays, airline booking systems down.
- India: Major airlines and IT firms.
- Israel: Emergency services, hospitals, and banks.
- Japan: Spring Japan airline experiencing issues.
- Malaysia: KTMB railway ticketing system issues.
- Netherlands: Schiphol airport, banks, and medical services disrupted.
- New Zealand: Banks, supermarkets, Auckland Transport, and Christchurch Airport.
- Philippines: Major banks, telecommunications, airlines, and government websites.
- South Africa: Banking issues.
- South Korea: Jeju Air experiencing issues.
- Singapore: Changi Airport delays, various service disruptions.
- Spain: National airport traffic control IT outage.
- Switzerland: Zurich Airport halted landings.
- United Kingdom: Airports, rail companies, NHS, and various services.
- United States: Airline ground stops, 911 service disruptions, and significant drops in Microsoft and CrowdStrike shares.

Our Recommendation

There are several methods to determine if your systems are affected by this update.

- Boot into Safe Mode and check the CrowdStrike Falcon sensor version. The problematic update seems to be affecting various sensor versions, including version 6.58.
- Check the installation date of the CrowdStrike Falcon sensor. If it coincides with the onset of BSOD issues (around July 19, 2024), it's likely to be the cause.

Look for the specific BSOD error message "DRIVER_OVERRAN_STACK_BUFFER," which is associated with this issue.

- While CrowdStrike develops a permanent fix, some users have found success using the following temporary workaround:
- Boot Windows into Safe Mode or the Windows Recovery Environment
- Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
- Locate the file matching "C-00000291*.sys" and delete it
- Boot the host normally

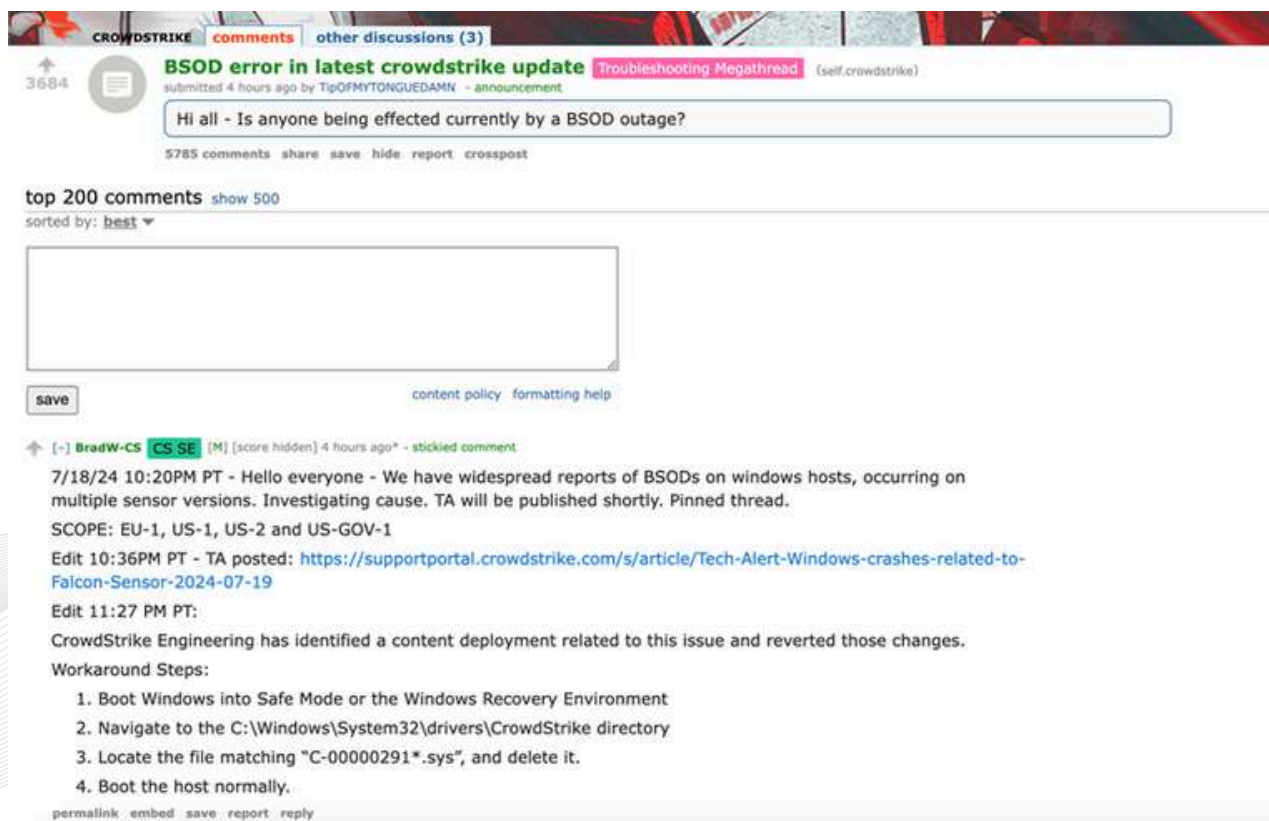



Fig: Recommendation of BSOD error


Conclusion

The recent CrowdStrike Falcon sensor incident highlights significant vulnerabilities and operational risks with automatic security updates, leading to widespread system failures, especially in enterprise environments. This underscores the need for rigorous testing and controlled deployment strategies of software updates. While CrowdStrike is addressing the issue, this incident emphasizes on the importance of balancing robust security with system stability and adopting best practices for software updates to prevent similar incidents in the future.



Contact Us

 arvind@atheniantech.com

 www.atheniantech.com

