Fixing CrowdStrike Issue on Windows

Author(s): Louis Ouellet

Recently, there was a significant issue involving CrowdStrike and Microsoft Windows. On July 19, 2024, CrowdStrike released a routine configuration update for their Falcon sensor software, which led to unexpected system crashes and blue screens of death (BSOD) on Windows systems. The update caused a logic error that corrupted essential system files, triggering widespread outages across various sectors, including healthcare, finance, and critical infrastructure.

Approximately 8.5 million Windows devices were affected, representing less than 1% of all Windows machines globally. The issue primarily impacted systems running the Falcon sensor for Windows version 7.11 and above that were online between 04:09 UTC and 05:27 UTC on the day of the update. The problem was particularly severe for devices with Windows BitLocker encryption enabled, as recovery required an encryption key often stored on servers that were also affected.

To mitigate the issue, users were advised to boot into Safe Mode or the Windows Recovery Environment and delete specific corrupted files from the CrowdStrike directory. CrowdStrike has since rolled back the problematic update and provided manual remediation steps to help affected users restore their systems. They are also conducting a thorough root cause analysis to prevent similar incidents in the future.

Solution

1. Boot the system into safe mode
2. Using a command-prompt or an explorer window, navigate to %windir%\System32\drivers\CrowdStrike
3. Delete all files starting by C-00000291 with the .sys extension
4. Reboot Windows in normal mode

Tagswindowssecuritycyber-securitycrowdstrikeoutagekernel

- Twitter
- Facebook
- LinkedIn
- Reddit
- Telegram
- Email

From:
https://laswitchtech.com/ - **LaswitchTech**

Permanent link:
https://laswitchtech.com/en/blog/2024/07/23/crowdstrike

Last update: **2024/11/07 11:10**