THREAT ADVISORY *CRITICAL*

July 19, 2024

CrowdStrike Causing Widespread Global Outages

SUMMARY

An update pushed out by CrowdStrike within the past 12 hours has caused widespread outages to Windows environments where CrowdStrike is installed. This was not an elective update and therefore was applied to every endpoint that had internet connectivity at the time. The impact this update caused the infamous Blue Screen of Death (BSOD) and will require manual intervention at every device.

IMPACT

Millions of end points globally were rendered inoperable, ranging from the 3 largest airlines, delaying flights, hospital networks, government agencies, and news networks. Any endpoint with CrowdStrike installed that has had internet connectivity within the past 12 hours is likely affected.

- End-points running older Windows 7 and 2008 R2 were not impacted
- End-points running Mac or Linux were not impacted.

The channel file “C-00000291*.sys” with a timestamp of 0409 UTC is the problem.

SOLUTION

Windows Endpoint (BitLocker not enabled)

1. "Boot Windows into Safe Mode or the Windows Recovery Environment
2. Use Windows Explorer or the Command Prompt to "Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
3. "Locate the file matching 'C-0000029*.sys', and delete it.
4. "Boot the host normally."

Windows Endpoint (BitLocker enabled)

1. Boot Windows into Safe Mode or the Windows Recovery Environment
2. Navigate to Troubleshoot > Advanced Options > Startup Settings
3. Press “Restart”
4. Skip the BitLocker recovery key prompt by pressing “Esc”
5. Skip the next BitLocker recovery key prompt by selecting “Skip This Device”, in the bottom right
6. Navigate to Troubleshoot > Advanced Options > Command Prompt
7. Type “bcdedit /set {default} safebook minimal”, then press “Enter”
8. Go back to the WinRE main menu and select “Continue”
9. The device may cycle 2 to 3 times
10. If booted into Safe Mode, log in as usual
11. Use Windows Explorer to "Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
12. "Locate the file matching 'C-00000291*.sys', and delete it.
13. Open Command Prompt as Administrator
14. Type “bcdedit /deletevalue {default} safeboot”. Then Press “Enter”
15. Restart as normal

Cloud Environment

Option 1

1. Detach the operating system disk volume from the impacted virtual server
2. Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
3. Attach/mount the volume to to a new virtual server
4. Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
5. Locate the file matching "C-00000291*.sys", and delete it.
6. Detach the volume from the new virtual server
7. Reattach the fixed volume to the impacted virtual server

Option 2

1. Roll back to a snapshot prior to 0409 UTC

REFERENCES

1. https://mashable.com/article/crowdstrike-crash-microsoft-outage-bsod-fix
2. https://www.wired.com/story/microsoft-windows-outage-crowdstrike-global-it-probems/
3. https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/