CENTRE FOR CYBERSECURITY BELGIUM

FLASH ALERT: LATEST UPDATE OF CROWDSTRIKE AGENT CAUSING BSOD LOOP ON WINDOWS!

Version: 1.0

Affected software: CrowdStrike Agent

Date:19/07/2024

Please distribute this information to your peers to inform as many companies as possible!

Risks

The CCB received information that the update for csagent.sys from CrowdStrike is causing blue screen loops. (BSOD) CCB recommends not to execute the update for the CrowdStrike agent until a verified fix is available.

Message from CrowdStrike

The faulty channel file 291 has been reverted and we hope that this will mitigate further expansion. For already crashing systems, some are rebooting to a normal working state, and we believe they should pick the new channel file 3) Some systems are just loop crashing and might need a manual intervention.

If your systems are loop crashing, they might need manual intervention.

Workaround Steps for individual hosts:

Warning: Bitlocker-encrypted hosts may require a recovery key. Make sure you have this information before you proceed.

1. Boot Windows into Safe Mode
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory in Explorer
3. Locate file “C-00000291-00000000-00000032.sys” file, right click and rename it to “C-00000291-00000000-00000032.renamed” (version might be different for your host)
4. Boot the host normally.

Workaround Steps for public cloud or similar environment:

- Detach the operating system disk volume from the impacted virtual server
- Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
- Attach/mount the volume to a new virtual server:
- Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
- Locate the file matching “C-00000291*.sys” and delete it.
- Detach the volume from the new virtual server
- Reattach the fixed volume to the impacted virtual server

TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

Contact

If you have any questions or need further assistance, please contact intelligence@ccb.belgium.be.

TLP:CLEAR