(https://www.crowdstrike.com/)

Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19

Cloud: US-1 EU-1 US-2

Published Date: Jul 19, 2024

Summary

- CrowdStrike is aware of reports of crashes on Windows hosts related to the Falcon Sensor.

Details

- Symptoms include hosts experiencing a bugcheck\blue screen error related to the Falcon Sensor.
- Windows hosts which have not been impacted do not require any action as the problematic channel file has been reverted.
- Windows hosts which are brought online after 0527 UTC will also not be impacted
- Hosts running Windows7/2008 R2 are not impacted.
- This issue is not impacting Mac- or Linux-based hosts
- **Channel file "C-00000291*.sys" with timestamp of 0527 UTC or later is the reverted (good) version.**
- **Channel file "C-00000291*.sys" with timestamp of 0409 UTC is the problematic version.**

Current Action

- CrowdStrike Engineering has identified a content deployment related to this issue and reverted those changes.
- If hosts are still crashing and unable to stay online to receive the Channel File Changes, the following steps can be used to workaround this issue:

Workaround Steps for individual hosts:

- Reboot the host to give it an opportunity to download the reverted channel file. If the host crashes again, then:
  - Boot Windows into Safe Mode or the Windows Recovery Environment
    - Note: Putting the host on a **wired network** (as opposed to WiFi) and using **Safe Mode with Networking** can help remediation.
  - Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
  - Locate the file matching “C-00000291*.sys”, and delete it.
  - Boot the host normally.

Note: **Bitlocker-encrypted hosts may require a recovery key**.

Workaround Steps for public cloud or similar environment including virtual:

Option 1:

- 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 to a new virtual server
- Navigate to the %WINDIR%\\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

Option 2:

- Roll back to a snapshot before 0409 UTC.

AWS-specific documentation:

- To attach an EBS volume to an instance (https://docs.aws.amazon.com/ebs/latest/userguide/ebs-attaching-volume.html#:~:text=To%20attach%20an%20EBS%20volume,and%20choose%20Actions%2C%20Attach%20volume)
- Detach an Amazon EBS volume from an instance (https://docs.aws.amazon.com/ebs/latest/userguide/ebs-detaching-volume.html)

Azure environments:

Pease see this Microsoft article (https://azure.status.microsoft/en-gb/status).

Latest Updates

- 2024-07-19 05:30 AM UTC | Tech Alert Published.
- 2024-07-19 06:30 AM UTC | Updated and added workaround details.
- 2024-07-19 08:08 AM UTC | Updated
- 2024-07-19 09:45 AM UTC | Updated
- 2024-07-19 11:49 AM UTC | Updated

Support

- Find answers and contact Support with our Support Portal (https://supportportal.crowdstrike.com/s/)