Windows crashes related to Falcon Sensor

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
- 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 workaround steps below can be used.
- We assure our customers that *CrowdStrike is operating normally and this issue does not affect our Falcon platform systems*. If your systems are operating normally, there is no impact to their protection if the Falcon Sensor is installed. Falcon Complete and Overwatch services are not disrupted by this incident.

Query to identify impacted hosts via Advanced event search

Please see this KB article: How to identify hosts possibly impacted by Windows crashes

Dashboard

Similar to the above-referenced query, a Dashboard is now available that displays Impacted channels and CIDs and Impacted Sensors. Depending on your subscriptions, it's available in the Console menu at either:

- Next-Gen SIEM > Dashboard or;
- Investigate > Dashboards

Note:

- The Dashboard cannot be used with the "Live" button

Automated Recovery Articles:

- Automated Recovery from Blue Screen on Windows Instances in GCP

Workaround Steps for individual hosts:

- Reboot the host to give it an opportunity to download the reverted channel file. We strongly recommend putting the host on a wired network (as opposed to WiFi) prior to rebooting as the host will acquire internet connectivity considerably faster via ethernet.
- 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
        - Windows Recovery defaults to X:\windows\system32
            - Navigate to the appropriate partition first (default is C:\), and navigate to the crowdstrike directory:
                - C:
                - cd windows\system32\drivers\crowdstrike
        - Note: On WinRE/WinPE, navigate to the Windows\System32\drivers\CrowdStrike directory of the OS volume
    - Locate the file matching “C-00000291*.sys”, and delete it.
        - Do not delete or change any other files or folders
    - Cold Boot the host
        - Shutdown the host.
        - Start host from the off state.

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:

- How do I recover AWS resources that were affected by the CrowdStrike Falcon agent?

Azure environments:

- Please see this Microsoft article.

User Access Recovery Key in the Workspace ONE Portal:

When this setting is enabled, users can retrieve the BitLocker Recovery Key from the Workspace ONE portal without the need to contact the HelpDesk for assistance. To turn on the recovery key in the Workspace ONE portal, follow the next steps. Please see this Omnissa article for more information.

Windows encryption management via Tanium:

- Please see this Tanium article for more information.

BitLocker recovery via Citrix:

- Please see this Citrix Article for more information.

BitLocker recovery-related KBs:

- BitLocker recovery in Microsoft Azure
- BitLocker recovery in Microsoft environments using SCCM
- BitLocker recovery in Microsoft environments using Active Directory and GPOs
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager
- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central
- BitLocker recovery in Microsoft environments using IBM BigFix

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
- 2024-07-19 11:55 AM UTC | Updated
- 2024-07-19 12:40 PM UTC | Updated, added query
- 2024-07-19 15:28 PM UTC | Updated
- 2024-07-19 16:30 PM UTC | Updated
- 2024-07-19 17:00 PM UTC | Updated
- 2024-07-19 17:55 PM UTC | Updated
- 2024-07-19 19:55 PM UTC | Updated
- 2024-07-19 20:26 PM UTC | Updated AWS Link
- 2024-07-20 00:05 AM UTC | Updated, added GCP automated recovery
- 2024-07-20 01:40 AM UTC | Updated, added dashboard and windows details

Support

- Technical details on outage
- Find answers and contact Support with our Support Portal