(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
- 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.**
  - Note: It is normal for multiple **"**C-00000291*.sys files to be present in the CrowdStrike directory - as long as *one* of the files in the folder has a timestamp of 0527 UTC or later, that will be the active content.

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

```
// Get ConfigStateUpdate and SensorHeartbeat events
#event_simpleName=/^(ConfigStateUpdate|SensorHeartbeat)$/ event_platform=Win
// Narrow search to Channel File 291 and extract version number; accept all SensorHeartbeat events within
impact window
| case{
    #event_simpleName=ConfigStateUpdate | regex("\|1,123,(?<CFVersion>.*?)\|", field=ConfigStateData,
strict=false) | parseInt(CFVersion, radix=16);
    #event_simpleName=SensorHeartbeat | rename([[@timestamp, LastSeen]]);
}


| case{
    #event_simpleName=ConfigStateUpdate | @timestamp>1721362140000 AND @timestamp < 1721366820000 |
CSUcounter:=1;
    #event_simpleName=SensorHeartbeat | LastSeen>1721362140000 AND LastSeen<1721366820000 | SHBcounter:=1;
    *;
}
| default(value="0", field=[CSUcounter, SHBcounter])
// Make sure both ConfigState update and SensorHeartbeat have happened
| selfJoinFilter(field=[cid, aid, ComputerName], where=[{ConfigStateUpdate}, {SensorHeartbeat}])
// Aggregate results
| groupBy([cid, aid], function=([{selectFromMax(field="@timestamp", include=[CFVersion])},
{selectFromMax(field="@timestamp", include=[@timestamp]) | rename(field="@timestamp", as="LastSeen")},
max(CSUcounter, as=CSUcounter), max(SHBcounter, as=SHBcounter)]), limit=max)
```

```
// Perform check on selfJoinFilter
| CFVersion=* LastSeen=*
// Calculate time between last seen and now
| LastSeenDelta:=now()-LastSeen
// Optional threshold; 3600000 is one hour
| LastSeenDelta>3600000
// Calculate duration between last seen and now
| LastSeenDelta:=formatDuration("LastSeenDelta", precision=2)
// Convert LastSeen time to human-readable format
| LastSeen:=formatTime(format="%F %T", field="LastSeen")
// Enrich aggregation with aid_master details
| aid=~match(file="aid_master_main.csv", column=[aid])
| aid=~match(file="aid_master_details.csv", column=[aid], include=[FalconGroupingTags, SensorGroupingTags])
// Convert FirstSeen time to human-readable format
| FirstSeen:=formatTime(format="%F %T", field="FirstSeen")


// Move ProductType to human-readable format and add formatting
| $falcon/helper:enrich(field=ProductType)
| drop([Time])
| default(value="-", field=[MachineDomain, OU, SiteName, FalconGroupingTags, SensorGroupingTags],
replaceEmpty=true)
| case{
    CSUcounter=0 AND SHBcounter=0 | Details:="OK: Endpoint did not receive channel file during impacted window.
Endpoint was offline.";
    CSUcounter=0 AND SHBcounter=1 | Details:="OK: Endpoint did not receive channel file during impacted window.
Endpoint was online.";
    CSUcounter=1 AND SHBcounter=1 | Details:="CHECK: Endpoint received channel file during impacted window.
Endpoint was online. Endpoint has not been seen online in past hour.";
}
```

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
    - 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.
  - 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:

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

Bitlocker recovery-related KBs:

- BitLocker recovery in Microsoft Azure (/s/article/ka16T000001tlmZQAQ)
- BitLocker recovery in Microsoft environments using SCCM (/s/article/ka16T000001tlmeQAA)
- BitLocker recovery in Microsoft environments using Active Directory and GPOs (/s/article/ka16T000001tlmjQAA)
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager (/s/article/ka16T000001tlmtQAA)
- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central (/s/article/ka16T000001tln8QAA)
- BitLocker recovery in Microsoft environments using IBM BigFix (/s/article/ka16T000001tlnSQAQ)

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 03:28 PM UTC | Updated

Support

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