Repairing Falcon Windows Sensors

Published Date: Jul 25, 2024

Introduction

This document will show you how to repair a broken sensor if you either deleted or modified the folder `C:\Windows\System32\drivers\CrowdStrike` or its content as a response to the Falcon Content Issue . Do not use this process if your sensor is currently operational or when you want to upgrade.

Important Note: If the host(s) was affected by the Falcon Content Issue ensure that the problematic Channel File 291 is deleted before progressing with the repair. If the channel file is not removed prior to repair, the machine will experience the BSOD loop again.

Falcon sensor status can be viewed on the the windows system from the “Falcon Status Icon”:

- The system tray icon will be grayed out and shows “Driver Status: Stopped” and “Service Status: Running”

From command prompt, the output for STATE will show “STOPPED” for one or both of the following:

- sc.exe query csagent
- sc.exe query csfalconservice

Prerequisites

- User has an administrative account that has rights to install Falcon.
- Falcon sensor installer is available either locally on the host or on a UNC path. The same sensor version installer should always be used
    - The correct version of the sensor installer for your cloud can be downloaded from:
        - US-1 sensor downloads
        - US-2 sensor downloads
        - EU-1 sensor downloads
        - GOV-1 sensor downloads

Repairing Falcon Sensor for Windows

Manual Repair:

If you have a small number of repairs, manual installation might be your best option.

- Use the Google Chrome browser to download the sensor installer from the links provided in the *Prerequisites* section above.
- Installer file names may vary based on the cloud your CID resides
    - US-1 = WindowsSensor.exe
    - US-2 = WindowsSensor.MaverickGyr.exe
    - EU-1 = WindowsSensor.LionLanner.exe
    - GOV-1 = WindowsSensor.GovLaggar.exe
- Place the installation file in the **`C:\Temp`** directory
- Open command prompt with Administrator privileges and run the following command:

    - `C:\Temp\<installation_file.exe> MAINTENANCE_TOKEN=<maintenance token> /repair /silent /forcedowngrade /norestart`
    - If the %SystemDrive%\Program Files\CrowdStrike directory or files located within have been deleted, you must include the MAINTENANCE_TOKEN.
    - If the %SystemDrive%\Windows\System32\drivers\CrowdStrike directory or files located within have been deleted, the MAINTENANCE_TOKEN can be omitted.
    - The %SystemDrive% variable is commonly set to c:, but can vary in some environments.

Automatic Repair:

To automate silent repair on many devices, including using a deployment tool such as Windows System Center Configuration Manager (SCCM), complete these steps:

- Use the Google Chrome browser to download the sensor installer from the links provided in the *Prerequisites* section above.
- Installer file names may vary based on the cloud your CID resides
    - US-1 = WindowsSensor.exe
    - US-2 = WindowsSensor.MaverickGyr.exe
    - EU-1 = WindowsSensor.LionLanner.exe
    - GOV-1 = WindowsSensor.GovLaggar.exe

- Run or configure your deployment tool to use this command, replacing `<installer_filename>` with the name if the install file you downloaded:
    - `<installation_file.exe> MAINTENANCE_TOKEN=<maintenance token> /repair /silent /forcedowngrade /norestart`
    - If the %SystemDrive%\Program Files\CrowdStrike directory or files located within have been deleted, you must include the MAINTENANCE_TOKEN.
    - If the %SystemDrive%\Windows\System32\drivers\CrowdStrike directory or files located within have been deleted, the MAINTENANCE_TOKEN can be omitted.
    - The %SystemDrive% variable is commonly set to c:, but can vary in some environments.

NOTE: If deploying automatic repair at scale. Use conditional checks to only repair hosts that are in a broken state. Running repair on hosts which are operating correctly should not be done.

Example conditional check:

Check if the following directories do not exist

- `%SystemDrive%\Windows\System32\drivers\CrowdStrike`
- `%SystemDrive%\Program Files\CrowdStrike`

Check if the following file does not exist

- `%SystemDrive%\Windows\System32\drivers\CrowdStrike\CSAgent.sys`
- `%SystemDrive%\Program Files\CrowdStrike\CSFalconService.exe`

Verifying Deployment

Falcon console

After the sensor is repaired, the host will connect to the Falcon Cloud. You can confirm a sensor installation by reviewing your hosts directly or checking the last seen from the Falcon Console:

- Host Setup & Management -> Host Management
- Use the Hostname Filter to identify your device
- Check the “Last Seen” column the timestamp should be from the last few minutes

Host

If you have remote access or direct access to the host you can also run the following commands from command prompt:

To verify the sensor state:

- sc.exe query csagent
- Output for STATE should show “4 RUNNING”

To verify the CSFalconService state:

- sc.exe query csfalconservice
- Output for STATE should show: “4 RUNNING”