CrowdStrike Automated Fix

On July 21, CrowdStrike began offering an additional remediation option for the Falcon Content Update for Windows Hosts issue.

This is separate to the CrowdStrike & Microsoft recovery tool that has also been published. This remediation uses Falcon's existing built-in quarantine functionality affected hosts. It is only applicable to affected hosts that can establish a network connection to the CrowdStrike cloud.

This remediation is available to all CrowdStrike customers who **choose to opt in**, this process is not automatic.

Please note that if you currently have an open ticket with CrowdStrike for this issue, this opt-in can be skipped.

We recommend you continue any manual remediation efforts that are ongoing as this process will not adversely affect those steps and will work in conjunction with those efforts.

How to opt in to remediation

Please have your Falcon Administrator create a Support case on our Support Portal at: https://supportportal.crowdstrike.com/s/cases with the following information:

- Case Title: Falcon Channel File Remediation
- In the Description, include the following:
  - Change Authorization: I authorize CrowdStrike Support to perform channel file remediation on my CID list
  - CID(s): Please include one or more CIDs
- Solution: Falcon Platform
- Falcon Product Area: Sensors - Windows OS Platforms
- Falcon Topic: Other (Window)

How the remediation works

This remediation option includes the following steps:

1. A Falcon Administrator requests the remediation via CrowdStrike Support ticket (outlined above). This will attempt to remediate all impacted hosts for a given customer environment (Customer ID / CID).
2. CrowdStrike Support will initiate the remediation targeted at the requested customer environment (CID). This remediation's only effect is to quarantine the problematic configuration file (also called a "channel file") that caused the content issue on July 19, 2024.
3. CrowdStrike support will apply the remediation and will provide an update in the case once completed.
4. You can then reboot the affected hosts to recover.
5. When each targeted Windows host connects to the CrowdStrike cloud, the problematic channel file is quarantined on that host.
    a. When the channel file is quarantined, it is moved from its current directory to a designated quarantine directory on the host.
    b. This means the channel file can no longer cause system crashes, which remediates the issue on targeted hosts.
6. After the problematic channel file is quarantined, the host may still BSOD once or twice. There's a race between the bad content being quarantined and the bad content being processed and activated in the sensor.
    a. If the host is no longer experiencing BSOD, the remediation action was successful.
7. Optional: an account administrator can delete the quarantined files using the Falcon console. For instructions on deleting quarantined files, see our Quarantined File documentation.

Recommendations

For best results there are some steps that will improve the effectiveness of the solution by allowing the sensor to connect to the CrowdStrike as early as possible in the boot process:

- Connect the host with a wired ethernet connection to avoid latency on Wi-Fi networks.
- Minimise load on the WAN connection (limit video streaming, VOIP sessions, etc) wherever possible.

Frequently Asked Questions

- Can this remediation cause destructive action on unaffected hosts?

    - The remediation only targets the specific problematic channel file. No other files can be quarantined by this remediation.
    - If a targeted host did not have the problematic channel file, no action will be taken on that host.
    - If a targeted host no longer has the problematic channel file (for example, if it was remediated manually), no action will be taken on that host. This host is no longer affected by the content issue.
- Will I see quarantine events in my console?
    - Yes, there are some cases in which the file is successfully quarantined, however the quarantine event does not always appear in the Falcon console. In these circumstances you can validate the quarantined file in the CrowdStrike quarantine directory on the host. You may receive notification emails based on your configuration settings. Successful remediation will result in the host returning to a healthy state.
- Do I need to delete the channel file after it has been quarantined?
    - No, but it is recommended. Even if a problematic channel file is released, the Falcon sensor does not use the problematic channel file if at least one newer channel file has been retrieved from the CrowdStrike cloud.
- How long does the remediation take to remediate the host of an affected machine?
    - After support responds to the request that reboots can begin on affected hosts, it can vary depending on how long it takes to receive the quarantine instructions after reboot. For certain hosts, it can take multiple reboots and machines may continue to remediate over time.

If remediation is not successful

In some cases, attempting additional reboots can be successful. This remediation relies on the Falcon sensor contacting the cloud and applying the quarantine before the problematic channel file can trigger a system crash.

Each reboot is another attempt at reproducing a favourable outcome.

For the latest information and alternate remediation options, see CrowdStrike's ongoing information hub which includes recovery instructions. New instructions are being added continuously to assist in manual recovery: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/