

REMEDIATION AND GUIDANCE HUB: FALCON CONTENT UPDATE FOR WINDOWS HOSTS

Statement From Our CEO

Technical Details

How Do I Identify Impacted Hosts?

How Do I Remediate Impacted Hosts?

How Do I Recover Bitlocker Keys?

How Do I Recover Cloud-Based Environments?

Third Party Vendor Information

VIDEO: CrowdStrike Host Self Remediation For Remote Users

Additional Resources

Page last updated 2024-07-23 0740 UTC

Updated 2024-07-22 2237 UTC

CrowdStrike tested an update to the [remediation that was deployed on Friday, July 19, 2024 05:27 UTC](#). The update has accelerated our ability to remediate hosts. Customers are encouraged to follow the Tech Alerts for latest updates as they happen.

We have [published a video](#) outlining the steps required to self-remediate impacted remote Windows laptops.

We will continue to provide updates here as information becomes available and new fixes are deployed.

CrowdStrike is actively assisting customers affected by a defect in a recent content update for Windows hosts. Mac and Linux hosts were not impacted. The issue has been identified and isolated, and a fix has been deployed. This was not a cyberattack.

Customers are advised to check the support portal for updates. We will also continue to provide the latest information here and on our blog as it's available. We recommend organizations verify they are communicating with CrowdStrike representatives through official channels.

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.

We understand the gravity of this situation and are deeply sorry for the inconvenience and disruption. Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

Statement from our CEO

Sent 2024-07-19 1939 UTC

Valued Customers and Partners,

I want to sincerely apologize directly to all of you for the outage. All of CrowdStrike understands the gravity and impact of the situation. We quickly identified the issue and deployed a fix, allowing us to focus diligently on restoring customer systems as our highest priority.

The outage was caused by a defect found in a Falcon content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

We are working closely with impacted customers and partners to ensure that all systems are restored, so you can deliver the services your customers rely on.

CrowdStrike is operating normally, and this issue does not affect our Falcon platform systems. There is no impact to any protection if the Falcon sensor is installed. Falcon Complete and Falcon OverWatch services are not disrupted.

We will provide continuous updates through our Support Portal at <https://supportportal.crowdstrike.com/s/login/>.

We have mobilized all of CrowdStrike to help you and your teams. If you have questions or need additional support, please reach out to your CrowdStrike representative or Technical Support.

We know that adversaries and bad actors will try to exploit events like this. I encourage everyone to remain vigilant and ensure that you're engaging with official CrowdStrike representatives. Our blog and technical support will continue to be the official channels for the latest updates.

Nothing is more important to me than the trust and confidence that our customers and partners have put into CrowdStrike. As we resolve this incident, you have my commitment to provide full transparency on how this occurred and steps we're taking to prevent anything like this from happening again.

George Kurtz

CrowdStrike Founder and CEO

Technical Details

- Technical Details on the outage can be found [here](#): [Read the blog Published 2024-07-20 0100 UTC](#)
- 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.
- CrowdStrike has identified the trigger for this issue as a Windows sensor related content deployment and we have reverted those changes. The content is a channel file located in the %WINDIR%\System32\drivers\CrowdStrike directory.
 - Channel file "C-00000291".sys" with timestamp of 2024-07-19 0527 UTC or later is the reverted (good) version.
 - Channel file "C-00000291".sys" with timestamp of 2024-07-19 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 05:27 UTC or later, that will be the active content.
- 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.

Non-Impacted Hosts

- Windows hosts which are brought online after 2024-07-19 0527 UTC will not be impacted
- Windows hosts installed and provisioned after 2024-07-19 0527 UTC are not impacted [Updated 2024-07-21 1436 UTC](#)
- This issue is not impacting Mac- or Linux-based hosts

How do I Identify Impacted Hosts?

How do I Identify Impacted Hosts via Advanced Event Search Query? [Updated 2024-07-22 0139 UTC](#)

The queries utilized by the dashboards are listed at the bottom of the appropriate dashboard manuals.

How do I Identify Impacted Hosts via Dashboard? [Updated 2024-07-23 0217 UTC](#)

An updated granular dashboard is available that displays the Windows hosts impacted by the content update defect described in this Tech Alert. See [Granular status dashboards to identify Windows hosts impacted by content issue \(v8.6\) \(pdf\)](#) or [log in to view in the support portal](#). Note that the queries utilized by the dashboards are listed at the bottom of the appropriate dashboard manuals.

How do I Remediate Impacted Hosts?

If hosts are still crashing and unable to stay online to receive the Channel File update, the remediation steps below can be used.

How do I Remediate Individual Hosts?

Updated 2024-07-21 0932 UTC

- 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 on reboot:
 - Updated 2024-07-22 1758 UTC
 - Option 1 – Build automated recovery ISOs with drivers
 - Follow the instructions for Building Falcon Windows Host Recovery ISOs in this manual (PDF) or [log in to view in the support portal](#). [Updated 2024-07-23 0740 UTC](#)
 - Note: Bitlocker-encrypted hosts may require a recovery key.
 - Option 2 – Manual process
 - Review the following video on [CrowdStrike Host Self Remediation for Remote Users](#). Follow the instructions contained within the video if directed to do so by your organization's IT department. [Updated 2024-07-22 1510 UTC](#)
 - Alternatively, please see this [Microsoft article](#) for detailed steps.
 - Note: Bitlocker-encrypted hosts may require a recovery key.

How do I Recover Bitlocker Keys? [Updated 2024-07-21 1810 UTC](#)

Bitlocker Recovery Manuals

Updated 2024-07-21 1810 UTC

Microsoft Azure

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 1810 UTC

SCCM

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 1810 UTC

Active Directory and GPOs

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 1810 UTC

Ivanti Endpoint Manager

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 1810 UTC

ManageEngine Desktop Central

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 1810 UTC

BigFix

(PDF) or [log in to view in the support portal](#).

Updated 2024-07-21 0023 UTC

Bitlocker recovery without recovery keys

(PDF) or [log in to view in the support portal](#).

Workspace ONE Portal

[Omniessa article](#)

Tanium

[Tanium article](#)

Citrix

[Citrix article](#)

How to Recover Cloud-Based Environment Resources

Cloud Environment Guidance

AWS

[AWS article](#)

Azure

[Microsoft article](#)

GCP

Updated 2024-07-22 1758 UTC

- See instructions for Manual Recovery from Blue Screen on Windows Instances in GCP (PDF) or [log in to view in the support portal](#)
- See [GCP CrowdStrike File Remediation Script](#) – provides a Python script customers can use to remediate impacted hosts residing in the GCP.

Public

Option 1:

Cloud/Virtual

- 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 a new virtual server
- Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
- Locate the files matching "C-00000291".sys", and delete them
- 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 2024-07-19 0409 UTC

Third Party Vendor Information [Updated 2024-07-20 2259 UTC](#)

Third Party Vendor

Guidance

Intel vPro technology remediation guide

[Remediate CrowdStrike Falcon® update issue on Windows systems with Intel vPro® technology](#)

Recovery for Rubrik customers

[CrowdStrike & Rubrik Customer Content Update Recovery For Windows Hosts](#)

Cohesity Support

[Cohesity's support for CrowdStrike's Falcon Sensor updates](#)

VIDEO: CrowdStrike Host Self-Remediation for Remote Users

This video outlines the steps required to self-remediate impacted remote Windows laptops. Follow these instructions if directed to do so by your organization's IT department.

[Watch the video now](#)

Additional Resources

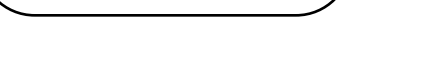
- [Statement from our CEO](#) [Published 2024-07-19 1919 UTC](#)
- [Falcon Sensor Content Issue Likely Used to Target CrowdStrike Customers](#) [Published 2024-07-19 2030 UTC](#)
- [Technical Details: Falcon Content Update for Windows Hosts](#) [Published 2024-07-20 0100 UTC](#)
- [Likely eCrime Actor Uses Filenames Capitalizing on Falcon Sensor Content Issues in Operation Targeting LATAM-based CrowdStrike Customers](#) [Published 2024-07-20 0145 UTC](#)
- [Threat Actor Uses Fake Recovery Manual to Deliver Unidentified Stealer](#) [Published 2024-07-22 1953 UTC](#)

Start your free trial now.

Total protection has never been easier. Take advantage of our free 15-day trial and explore the most popular solutions for your business:

- ★ Protect against malware with next-gen antivirus.
- ★ Get unrivaled visibility with USB device control.
- ★ Simplify your host firewall management.
- ★ Defeat adversaries with automated threat intelligence.

[Request free trial](#) →

 CROWDSTRIKE

[X](#) [f](#) [@](#) [in](#) [v](#)

New to CrowdStrike?

About the platform

Explore products

Services

Why choose CrowdStrike?

Company

About CrowdStrike

Careers

Events

Newsroom

Partners

CrowdStrike Marketplace

Learn with CrowdStrike

2024 Global Threat Report

Cybersecurity 101

Your Threat Landscape

Tech Center

View all resources

Contact us →

Experienced a breach? →