Update: Microsoft Releases Updated Recovery Tool To Mitigate CrowdStrike Falcon Agent Issue

Informational TLP:WHITE Alert ID : 8c7ef0bf Jul 22, 2024, 11:24 AM

Update July 22, 2024

Over the weekend, Microsoft released an updated USB recovery tool to address the CrowdStrike Falcon agent issue that is impacting Windows clients and servers. The signed Microsc

The tool offers two repair options: recovery from WinPE and recovery from safe mode.

Recovery from WinPE is recommended for quick system recovery without local admin privileges and requires a BitLocker recovery key. If you want to avoid entering recovery keys, you

In preparation for recovery, you should ensure access to BitLocker recovery keys for encrypted devices when using the WinPE option or obtain local administrator account credentials

Before deploying the solution, it is recommended that the recovery process on multiple devices be thoroughly tested before broad implementation.

After recovery, it is recommended to restore the original boot settings, especially for virtual machines, and to remove temporary firewall rules created for PXE recovery.

Microsoft has also offered an alternative to these solutions in cases where recovery from USB is not possible.

More detailed instructions are available here: New Recovery Tool To Help With CrowdStrike Issue Impacting Windows Endpoints.

As the situation evolves, Health-ISAC members should stay informed about any updates or additional guidance provided by Microsoft and CrowdStrike. Continuous monitoring and fee employed.

Health-ISAC has a dedicated CrowdStrike Slack Secure Chat channel set up where other members are discussing remediation efforts. The channel can be found here #crowdstrike_us

Health-ISACs Threat Operations Center (TOC) will continue to monitor the situation and provide updates as they are made available.

Update July 20, 2024

On July 20, 2024, Microsoft issued an updated Knowledge Base article, KB5042421, with additional step-by-step guidance is now available.

Microsoft has identified an issue impacting Windows endpoints that are running the CrowdStrike Falcon agent. These endpoints might encounter error messages 0x50 or 0x7E on

Microsoft has received reports of successful recovery from some customers attempting multiple restart operations on affected Windows endpoints.

Microsoft will continue to work with CrowdStrike to provide up-to-date mitigation information as it becomes available.

Health-ISAC has a dedicated CrowdStrike Slack Secure Chat channel set up where other members are discussing remediation efforts. The channel can be found here #crowdstrike

Health-ISACs Threat Operations Center (TOC) will continue to monitor the situation and provide updates as they are made available.

To mitigate this issue, follow these steps:

1. Start Windows into Safe Mode or the Windows Recovery Environment.
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
3. Locate the file matching “C-00000291*.sys” and delete it.
4. Restart the device.
5. Recovery of systems requires a Bitlocker key in some cases.

For Windows Virtual Machines running on Azure follow the mitigation steps in Azure status.

Additional details from CrowdStrike are available here: Statement on Windows Sensor Update - CrowdStrike Blog.

Microsoft Customers may attempt to restore their Cloud PC to a known good state prior to the release of the update (July 19, 2024) as documented here:
1. Enterprise: learn.microsoft.com/en-us/windows-365/enterprise/restore-overview
2. Business: learn.microsoft.com/en-us/windows-365/business/restore-overview

On July 19, Microsoft reported a worldwide outage affecting Windows users, which was caused by a faulty CrowdStrike Falcon sensor update. Windows users have reported experi

Health-ISAC has a dedicated CrowdStrike Slack Secure Chat channel set up where other members are discussing remediation efforts. The channel can be found here #crowdstrike

Health-ISACs Threat Operations Center (TOC) will continue to monitor the situation and provide updates as they are made available.

Additional Information

Impacted services may include but are not limited to the following:

- Microsoft Teams: Users may be unable to leverage Microsoft Teams functions, which include presence, group chats, and user registration.
- Microsoft 365 admin center: Admins may be intermittently unable to access the Microsoft 365 admin center, and any action may be delayed if it is not accessible.

The issue is limited to Windows, Mac and Linux hosts are not known to be impacted at this time. A possible workaround to the issue is to boot the affected machine in Safe Moc

Organizations worldwide, including critical infrastructure like airports and banks, are currently affected. Gatwick Airport has reported significant disruption due to the outages. Tl
and prepare for possible operational disruptions.

CrowdStrike has issued an official statement confirming that the outages were not a result of a cyberattack. The company claims they have isolated the issue and issued fixes. V
Microsoft’s mitigation efforts are available on the Microsoft service health status page.

Members are advised to follow updates on CrowdStrike’s website to minimize the risk of possible operational disruptions. More information is available in the CrowdStrike’s stat

Report Source(s)

Microsoft

Release Date

Jul 20, 2024, 11:59 PM

Reference | References

Microsoft Blog
Microsoft Cloud
Azure Status
Crowdstrike Falcon Guidance
Microsoft Blog
Microsoft Blog
CNN Money
Crowdstrike Falcon Guidance
Crowdstrike Falcon Guidance
Microsoft Blog

Tags

CrowdStrike, Outage, Microsoft

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile a

For Questions or Comments:

Please email us at toc@h-isac.org