TACTICAL REPORT: Millions of Microsoft Windows Device Outages Result From CrowdStrike Update

July 19, 2024

TLP: WHITE ○○○

Source: Statement on Falcon Content Update for Windows Hosts | CrowdStrike

If you are impacted by this outage, please contact CyberAlberta at CyberAlberta@gov.ab.ca so we can better track the impact to Albertan organizations, and pass along intelligence as it becomes available.

Overview:

A widespread technology outage attributed to a software update issued by CrowdStrike resulted in crashes of machines running the Microsoft Windows operating system. The outage has affected airlines, banks, broadcasters, IT service providers, and other businesses worldwide—including members of the CyberAlberta Community of Interest—causing significant disruptions.

Details:

- On 18 July 2024, CrowdStrike pushed an update to client devices using Falcon, a service provided by CrowdStrike which monitors an organization's devices for threats such as hacking attempts and viruses. Shortly after customers began noting outages.
- This update may result in a faulty channel file, which has caused impacted systems to crash and become stuck in a Blue Screen of Death boot loop.
- CrowdStrike has identified and isolated the issue and has stopped pushing the update to systems not yet patched. They have also deployed a fix; however, to implement the fix, impacted clients will need to use a manual workaround to get the fix to the affected devices.
- Given the nature of the fix, some cybersecurity experts suggest that it may be difficult to deploy the fix at large scale.

Recommended Actions:

- The workarounds suggested for public cloud or similar environments is to:
  1. Detach the operating system disk volume from the impacted virtual server
  2. Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
  3. Attach/mount the volume to a new virtual server

4. Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
5. Locate the file matching “C-00000291*.sys” and delete it.
6. Detach the volume from the new virtual server
7. Reattach the fixed volume to the impacted virtual server

OR

1. Roll back to a snapshot before 0409 UTC.

- The workaround recommended by CrowdStrike for individual hosts is to reboot the device to allow it to attempt to download the reverted channel file.
- CrowdStrike is recommending the following actions for systems that are impacted and crashing due to affected channel files:
  1. Boot Windows in Safe Mode or WRE.
  2. Go to C:\Windows\System32\drivers\CrowdStrike
  3. Locate and delete file matching "C-00000291*.sys"
  4. Boot normally.

  NOTE: Organizations which use Bitlocker may require a recovery key.
- Microsoft is suggesting the actions recommended here if you are running a Windows Client/ Server virtual machine.
- SANS is recommending that booting impacted systems in **Windows Safemode with Network** may fix the issue as it will negate CrowdStrike from starting but still allow the current version to be downloaded and applied, which should fix the issue.

Further Reading:

- Issue impacting CrowdStrike Falcon EDR | Canadian Centre for Cyber Security
- Global IT Outage Linked to Crowdstrike Software Issue Grounds Flights, Hits Banks and Businesses | Wall Street Journal
- Global IT Outage Live Updates: Microsoft and CrowdStrike Issues Affect Flights and Businesses | The New York Times
- 3 ways to fix CrowdStrike BSOD issue on Windows PCs| Windows Report

CYBER ALBERTA