Cyber Security Centre of Excellence
West Bengal

Department of Information Technology & Electronics
Government of West Bengal
https://cscoe.itewb.gov.in/

Alert on outage of Microsoft Windows

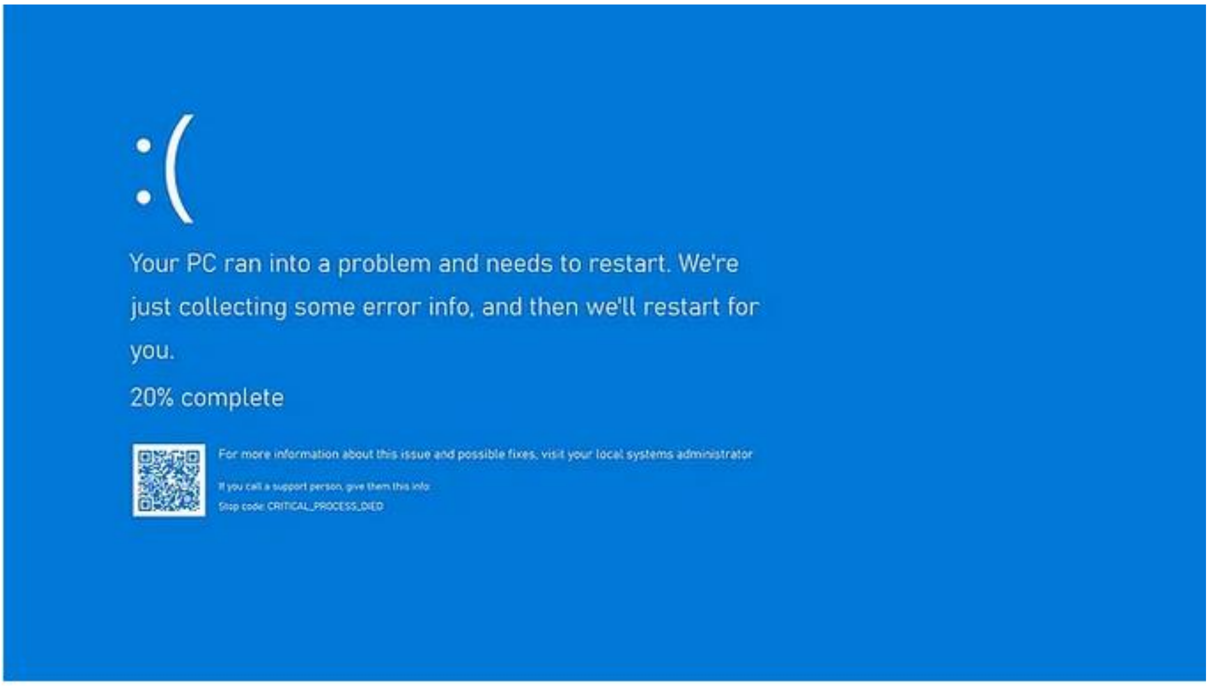
Overview

It was reported that millions of Windows users across the globe experienced unresponsiveness, startup failures and experienced a “Blue Screen of Death(BSOD)” on 19th July 2024 at 04:09 UTC. The incident was triggered due to recent update received in Crowd Strike agent “**Falcon Sensor**”. Consequently, the changes were reverted by the Team.

The Microsoft error was due to a patch update which affected on-premises and various cloud platforms. The critical sectors such as aviation, banking, healthcare, stock Markets etc were brought to standstill.

How it happened?

Crowd Strike Falcon is EDR(End point Detection and Response) Security system.**“Endpoint protection**” describes software that runs on local machines to ensure they do not execute malicious software or any unintended code.CrowdStrike updated its Falcon Sensor agent for Windows but a bug(logic error) in this update resulted in catastrophic system failure and BSOD.



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit your local systems administrator

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

Windows infamous blue screen of 19th July 2024

The blue screen of death problem “often indicates kernel-level conflicts or bugs, it is generally encountered in Windows systems. This error indicates that the system has malfunctioned, usually due to hardware or software issues.

Analysis:

The Crowd Strike Falcon Sensor's driver that runs in the kernel mode, has the highest privilege level on a computer system. They basically have a bug on process update. Their downloaded definition file is empty. When the Crowd Strike Falcon Sensor driver tries to process the empty file (file provided during update by CrowdStrike), it crashes the system due to a null pointer reference.

Due to security measure Crowd Strike Falcon declared their driver as a boot-start driver, so at every boot Crowd Strike Falcon was finding new updated definition file which was null and due to that system was trying to identify essential driver to boot and kept rebooting itself.

Steps to Resolve

The following steps can be used as work around for this issue:

- **Crowdstrike's Update – Quick Steps**

  Step 1: *Boot Windows into Safe Mode or WRE.*
  Step 2: *Go to C:\Windows\System32\drivers\CrowdStrike.*
  Step 3: *Locate and delete the file matching "C-00000291*.sys"*
  Step 4: *Boot normally.*

- **Microsoft Azure**

  ✓ Restore from Backup: In case customers have available backups, they should recover VM data from the backups. If the customer is using Azure Backup, they can get exact steps on how to restore VM data in the Azure portal.

  ✓ Offline OS Disk Repair: Alternatively, customers can attempt offline repair of the OS disk by attaching an unmanaged disk to the affected VM. Once attached, delete the following file:

  Windows/System/System32/Drivers/CrowdStrike/C00000291*.sys

  After deletion, reattach the disk to the original VM.

- The most up-to-date remediation information can be found on Crowdstrike blog/Support Portal.The root cause analysis is being done by CrowdStrike as the investigation progresses. (https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/)..

- Boot the machine into safe mode. This mode only loads a limited set of drivers and hopefully will allow you to log into the

- Blue Screen errors can stem from both hardware and software issues. If new hardware was added before the error, try removing it and restarting your PC. If restarting is difficult, start your PC in Safe Mode.

- Use the file manager to go to the path – "window\system32\drivers\crowdstrike".

- Find the file matching the pattern "C*" (followed by a bunch of zeros and then ".sys") and delete it.

- Reboot your system. The system should come up normally without the faulty update file.

- If none of those steps help to resolve your Blue Screen error, please try the Blue Screen Troubleshooter in the Get Help app:
    - In Windows, open Get Help.
    - In the Get Help app, type Troubleshoot BSOD error.
    - Follow the guided walk through in the Get Help app.

References:

- https://www.cyberpeace.org/resources/blogs/cyberpeace-alert-global-disruptions-as-crowdstrike-update-triggers-windows-bsod

- https://www.ndtv.com/world-news/windows-systems-restarting-throwing-blue-screen-of-death-due-to-crowdstrike-error-6138820#

- https://support.microsoft.com/en-gb/windows/start-your-pc-in-safe-mode-in-windows

- https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

- https://www.cert-in.org.in/

- https://www.nfsu.ac.in/

- https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/