Windows Computers Lead To 'Blue Screen Of Death' Due To CrowdStrike Error

sky news

We apologise for the interruption to this broadcast.
We hope to restore the transmission of Sky News shortly.

Report : CrowdStrike attack on July 19th.

What is CrowdStrike

- It is a cybersecurity company.
- It helps to secure environment
- Secure from hacaers/cyber stacks
- It is responsible for Data leakage protection & maintainence

So ,it is End point protection .

ISSUE:

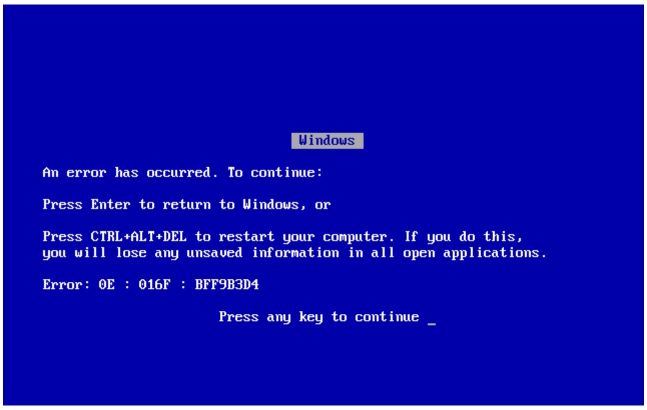
On July 19th, a faulty update from CrowdStrike's Falcon security software caused a widespread system outage.

Thousands of computers running Microsoft Windows and a cyber security program by CrowdStrike on Friday morning were suffering severe glitch, resulting in bug triggered Blue Screen of Death (BSOD) errors on Windows machines causing systems to crash.

What is BSOD

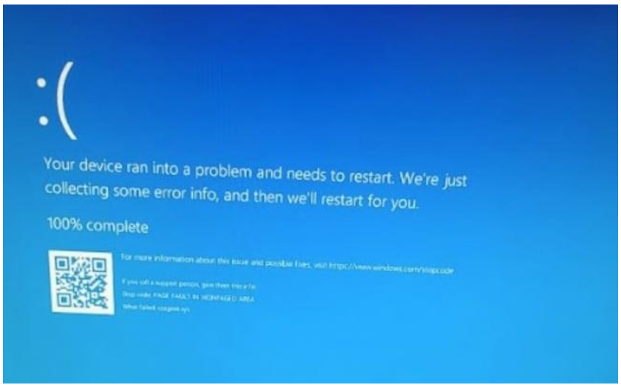
The Blue Screen of Death (BSOD), also known as a stop error, is a critical error screen displayed by Microsoft Windows. It essentially indicates a system crash where the operating system encounters a critical issue that prevents it from operating safely.

In general BSOD shows the type of error. Example :-



```
                              Windows
An error has occurred. To continue:

Press Enter to return to Windows, or

Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.

Error: 0E : 016F : BFF9B3D4

                       Press any key to continue _
```

shown ->



```
:(

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

100% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: PAGE FAULT IN NONPAGED AREA
What failed: csagent.sys
```

But rather showing type of error it throws device ran into problem

The issue has impacted potentially millions of people worldwide as airlines, airport authorities, banks, government organisations, private companies and municipal authorities scrambled to address the issue.

The Windows outage is so severe and widespread that many are attributing it to a cyberattack. However, CrowdStrike CEO has now issued a statement, saying that the Windows computers are glitching because of a bug and not cyber attack.

- This incident affected countries that rely heavily on Windows operating systems, are:

India,	Australia,	Japan,	Germany,
Britain,	New Zealand,	United States	

CrowdStrike's official statement: CrowdStrike blog

https://www.crowdstrike.com/blog/our-statement-on-todays-outage/

News article about the incident: India Today article

https://www.indiatoday.in/technology/news/story/crowdstrike-ceo-says-windows-bsod-is-not-a-cyber-attack-it-expert-calls-it-biggest-it-outage-in-history-2569152-2024-07-19

Impact:

The outage caused disruptions across various sectors, including:

Transportation: Thousands plus of flights were cancelled due to grounded airplanes.

Manual work is taken place

Large queue taken place by passengers

Media: Broadcasting stations were knocked off the air.

SKY NEWS stopped broadcast.

Finance: Effect on Banks and other financial institutions experienced service disruptions.

Effect on Atm

Healthcare: Access to healthcare services may have been impacted.

Hospitals switche to manual process

Government: Government agencies may have faced service interruptions.

➢ Solutions & Recovery for the CrowdStrike Incident

For Users:

- Boot windows machinein safe mode
- Delete files relate to crowdstrike
- System Backups
- Cloud-Based Alternatives
- Offline Functionality
- Stay updated

➢ Steps : for some computers

Turn on computer

Start tapping F8 (for other chech how to go to "recovery environment ") to get into safe mode or WRE -> then back up & run -> go to pc -> c drive ->windows -> scroll down -> system32 ->drivers-> look for "crowdStrike " folder -> delete -> C-00000291*.sys"

Once you delete file reboot normally

Report: CrowdStrike Incident (July 19, 2024) approx: 10 AM in India

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

https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

Analysis By-

Kundan kumar