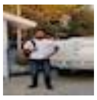
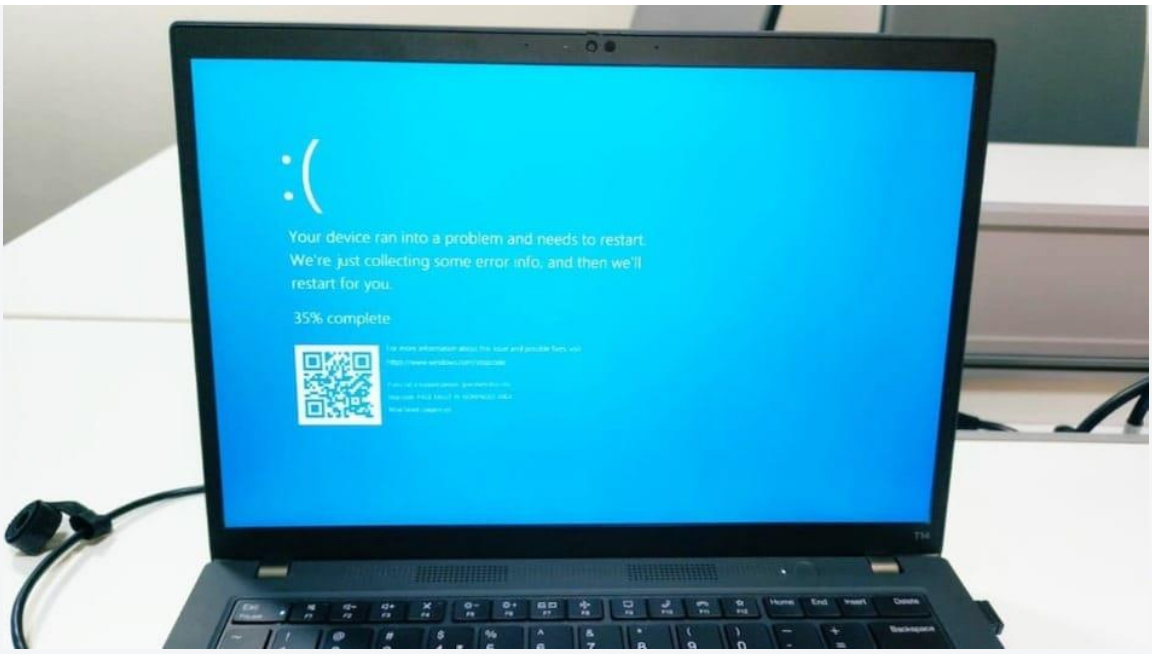
Microsoft outage: Crowdstrike reveals technical reasons behind one of the biggest outages of history

On July 19, 2024, many Windows users experienced the Blue Screen of Death due to a CrowdStrike update. This report details the incident, its impact, and how to resolve it.



Danny D'Cruze


:(
Your device ran into a problem and needs to restart.
We're just collecting some error info, and then we'll restart for you.
35% complete

Microsoft cloud outage, microsoft servers down, world, banks, airline flights,

On July 19, 2024, many Windows users were hit with the Blue Screen of Death (BSOD), leading to widespread disruptions. The cybersecurity company behind the entire fiasco, Crowdstrike has released a detailed report about the problem. An update from the company was the reason behind the outage. Here's a detailed breakdown of what happened and how to fix it.

On July 19, 2024, at 04:09 UTC, CrowdStrike released a sensor configuration update to Windows systems as part of their Falcon platform's ongoing operations. This update triggered a logic error, resulting in system crashes and the BSOD on affected systems.

Technical reasons behind the outage

The issue affected customers using Falcon sensor for Windows version 7.11 and above, who were online between 04:09 UTC and 05:27 UTC on July 19, 2024. Systems that downloaded the updated configuration during this period were susceptible to crashes.

The problematic update involved "Channel Files," which are part of Falcon's behavioural protection mechanisms. These files reside in the directory:

The specific file responsible was "C-00000291-.sys." This file controls how Falcon evaluates named pipe execution on Windows systems. The update aimed to target newly observed malicious named pipes but inadvertently caused a system crash due to a logic error.

George Kurtz, President & CEO of Crowdstrike had released a statement saying, "Crowdstrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This is not a security incident or cyberattack. The issue has been identified, isolated, and a fix has been deployed. We recommend customers use our support portal for updates and communicate with Crowdstrike representatives through official channels."

Sundareshwar K, Partner & Leader - Cybersecurity at PwC India said, This incident is a "black swan" event, highlighting the need for organisations to rethink their cybersecurity strategies beyond just technology.

Vishal Salvi, CEO of Quick Heal Technologies Limited said, this disruption serves as a wake-up call for businesses to prioritise proactive defence strategies and ensure comprehensive contingency plans, including regular data backups and robust disaster recovery strategies.