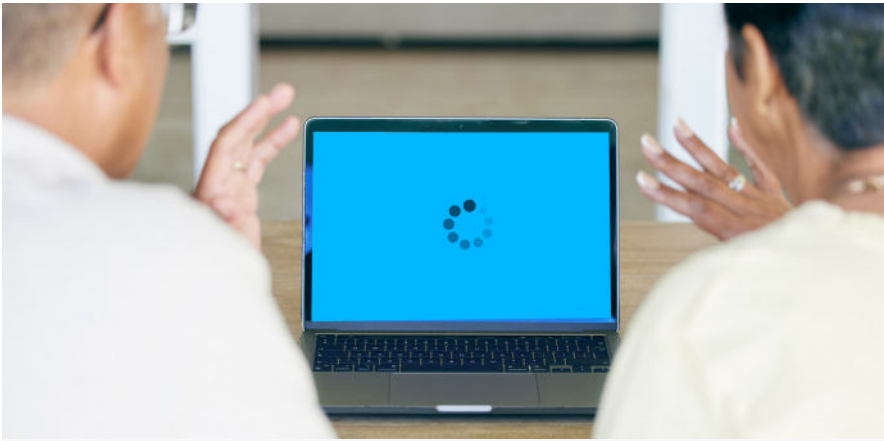


CrowdStrike:
Exploring the Outage
that Caused Chaos
Across the World

Reliable



A patch pushed by cybersecurity firm CrowdStrike in July 2024 caused an outage which affected millions of Windows devices all over the globe and caused them to become inoperable, presenting users with the dreaded 'Blue Screen of Death'.

CrowdStrike is a global leader in cybersecurity providing services to more than half of Fortune 1000 companies, and with a customer base that includes the likes of Intel, Salesforce, TUI, and Talk Talk.

What caused the outage?

The event was caused by CrowdStrike's Falcon Sensor tool which is used to detect cyberattacks.

A badly written configuration file, read by code that was not thoroughly tested, caused the tool to misbehave and attempt to access memory improperly. Normally, Windows would prevent a program from trying to do this. However, due to the high level of access to the operating system afforded to Falcon, Windows saw it as an internal error with no way to recover, resulting in the 'Blue Screen of Death'.

It's likely that the software had been tested with a valid configuration file, so that no issues were found at that time. Configuration files are frequently not tested, as they are not written as code. Once released, this combination of 'happy-path' testing and a false sense of security resulted in crashed systems.

How the events unfolded

Tools like CrowdStrike's Falcon Sensor are important for businesses to ensure they

are protected from online threats, and can change rapidly as new vulnerabilities are discovered. As such, remaining up-to-date is important to maximise effectiveness. Because of this, many companies have their security software set to automatically update as new releases are rolled out by the vendor.

At around 5:00am UK time, the broken update was pushed. This meant computers started becoming affected outside of normal business hours, when few people would have been available to stop the updates. Of course, even if the update had been pushed at a more favourable time, the failures would need to have been spotted immediately for application of the update to have been paused.

As computers were restarted, the result was a boot loop in which the system could never reach a stable state without manual intervention from a technician. The update was pulled within 90 minutes, but in that time an estimated 8.5 million computers had been affected.

Protecting your business



It's important to stay up to date, but events such as this highlight the necessity of building a strong and robust approach to protecting your business's digital systems. Organisations can protect themselves in two powerful ways to reduce their risk of being impacted by such events in the future...

1. Put yourself in control

Part of the reason Reliable customers suffered minimal disruption is due to our stringent patch management policies. These give us complete confidence that we're updating software in the best possible way. We put you in control. We also make use of N-able; a powerful security and estate management platform which ensures all patches are comprehensively tested before release.

2. Plan for the worst.

This event shows that even the largest companies can encounter catastrophic issues that impact operations. Be sure to do everything you can to ensure they don't become your issues. Make backups, and store them securely. Have a disaster recovery plan, and be confident it works. Improve your team's technical literacy and threat awareness, to ensure you can act when needed.

Reliable

For expert help protecting your systems and keeping your network operating as usual, contact us.

Call: 03333 1111 33

Email: hello@reliablenetworks.co.uk

Reliable

46-48 East Smithfield,
London E1W 1AW

www.reliablenetworks.co.uk