GMA NEWS ONLINE
YOUR NEWS AUTHORITY
(https://www.gmanetwork.com/news/)

SCITECH

Filtered by: Scitech

EXPLAINER: CrowdStrike identifies cause of global Microsoft outage

By Reuters

Published July 19, 2024 8:04pm

A cash register shows a blue screen at a grocery store affected by a cyber outage in Sydney, Australia July 19, 2024. REUTERS/Stella Qiu

LONDON - A global tech failure disrupted operations across multiple industries on Friday, halting flights and forcing a number of broadcasters off air, as the outage upended everything from banking to healthcare systems.

What happened?

CrowdStrike, a U.S. cybersecurity company, is among the most popular in the world, counting more than 20,000 subscription customers around the world.

According to an alert sent by CrowdStrike to its clients and reviewed by Reuters, its widely used "Falcon Sensor" software is causing Microsoft Windows to crash and display a blue screen, known informally as the “Blue Screen of Death”.

The alert, which was sent at 0530 GMT on Friday, also shared a manual workaround to resolve the issue.

Other Stories

PH banks hit by global Microsoft outage

(https://www.gmanetwork.com/news/money/companies/913970/ph-banks-digital-services-hit-by-global-microsoft-outage/story/)

Global Microsoft outage affects Cebu Pacific, AirAsia Philippines

(https://www.gmanetwork.com/news/money/companies/913963/microsoft-outage-disrupts-operations-of-cebu-pacific-airasia-philippines/story/)

Global cyber outage grounds flights, hits banks, telecoms, media

(https://www.gmanetwork.com/news/scitech/technology/913957/global-cyber-outage-grounds-flights-hits-media-financial-telecoms/story/)

Why did it happen?

"The damage to business processes at the global level is dramatic. The glitch is due to a software update of CrowdStrike's EDR product," said Omer Grossman, Chief Information Officer at identity security firm CyberArk.

EDR, or Endpoint Detection and Response, is a cybersecurity product that companies place on their clients' computers to help defend them from hackers. That software, which runs in the background on clients' machines, or endpoints, is used by cybersecurity firms to monitor for signs of attack on their clients' networks.

"It turns out that because the endpoints have crashed - the Blue Screen of Death - they cannot be updated remotely and the problem must be solved manually, endpoint by endpoint. This is expected to be a process that will take days," he added.

Who has been impacted?

The global tech outage (https://www.gmanetwork.com/news/scitech/technology/913957/global-cyber-outage-grounds-flights-hits-media-financial-telecoms/story/) has affected operations in different sectors internationally including at Spanish airports, U.S. airlines and Australian media and banks.

The governments of Australia, New Zealand, and a number of U.S. states are facing issues, while American Airlines AAL.O, Delta Airlines DAL.N, United Airlines (UAL.O), and Allegiant Air (ALGT.O grounded flights citing communication problems.

In Britain, Sky News, one of the country's major television news channels, was off air on Friday.

Why are so many impacted?

With the move to the cloud and with companies owning huge market shares, their software is running on millions of computers around the world.

"The damage to business processes at the global level is dramatic," said Grossman.

—**Reuters**

Tags: Crowdstrike (https://www.gmanetwork.com/news/tracking/crowdstrike/), cyber outage (https://www.gmanetwork.com/news/tracking/cyber_outage/), microsoft (https://www.gmanetwork.com/news/tracking/microsoft/)