



| Flash |

Global IT Outages Causing Significant Disruption to Multiple Industries

F-2024-07-19a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Cyber, Global, Information Technology

July 19, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on July 19, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Global IT Outages Causing Significant Disruption to Multiple Industries

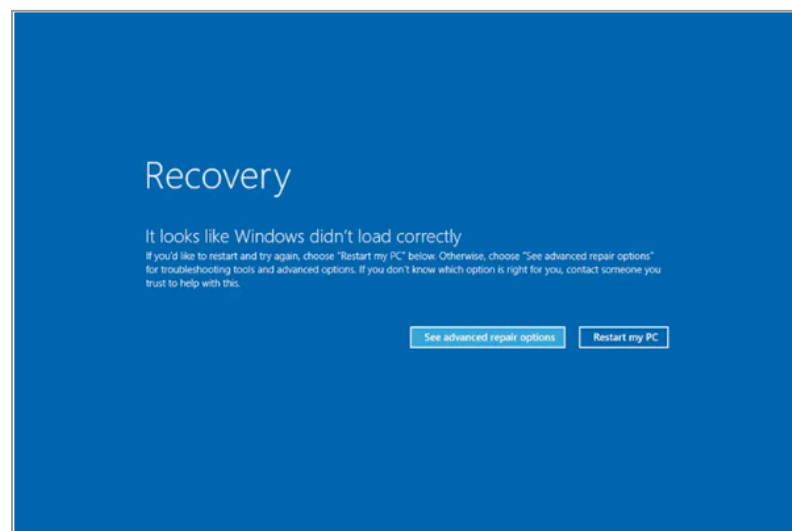
> Key Findings

- On July 18, 2024, a global Information Technology (IT) outage caused significant disruption to industries around the world, with thousands of Windows workstations and servers displaying a fatal system error message commonly referred to as the “blue screen of death.”
- The incident reportedly impacts Windows hosts that have installed CrowdStrike’s Falcon Sensor service; it does not affect all Windows devices.
- At the time of writing, the cause of the outage is not being treated as a cyberattack and is instead most likely to be a faulty or incorrectly deployed security update or a faulty channel file.
- The outage is known to have affected Windows devices across the world, with a significant impact across multiple industries—including, but not limited to—Energy, Finance, Healthcare, Media, Retail, and Travel.
- The current workaround provided by the vendor requires a physical presence at each device and almost certainly cannot be deployed remotely.

| Details

On July 18, 2024, a global IT outage caused significant disruption to industries around the world, with thousands of Windows workstations and servers displaying a fatal system error message commonly referred to as the “blue screen of death.”¹ The incident is reportedly impacting Windows hosts that have installed CrowdStrike’s Endpoint Detection and Response (EDR) Falcon Sensor service; the incident does not affect all Windows devices. At the time of writing, the cause of the outage is not being treated as a cyberattack and is instead most likely to be a faulty or incorrectly deployed security update or a faulty channel file.²

- Falcon is a widely deployed, high-privilege security tool used to monitor and detect system intrusions and take action to mitigate these threats.
- It is designed to have extensive access control capabilities on the devices it is installed upon.
- Reporting indicates that the error message is displayed upon booting the device.



“Blue Screen of Death” displayed on affected Windows devices

Source:

<https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue>

¹ <https://azure.status.microsoft.com/en-us/status>

² <https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/>

This is an ongoing incident, and the scale of the impact is still being assessed. The outage is known to have affected Windows devices across the world, including—but not limited to—North America, Europe, and the Asia-Pacific region. Just some of the affected industries include:

- Finance – Widespread disruption to financial and banking services, as well as global stock markets.³
- Healthcare – Significant impact on healthcare services and hospitals.
- Travel – Significant delays and suspension of services for trains and flights, including the closure of airports, citing communication issues.⁴⁵
- Media – Television networks temporarily stopped broadcasting.⁶ While service has been resumed, some are operating without broadcasting graphics.
- Retail – Disruption to payment systems.
- Energy – Disruption to energy and gas trading markets, significantly restricting the ability to buy and sell power.

At the time of writing, the workaround provided by the vendor requires a physical presence at each device and almost certainly cannot be deployed remotely. On July 19, 2024, CrowdStrike issued an advisory acknowledging the incident, stating that it is working on resolving the issue and providing a workaround for some affected devices. While the advisory was published behind a customer login page, it has since been posted widely in open sources.⁷ Users are advised to:

1. Boot Windows into Safe Mode or the Windows Recovery Environment.
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory.
3. Locate the file matching "C-00000291*.sys" and delete it.
4. Boot the host normally.

Currently, there is no workaround that can be deployed centrally, as the issue occurs upon booting the device and before the operating system has loaded. This will likely

³

[hXXps://www.theguardian\[.\]com/business/live/2024/jul/19/retail-sales-great-britain-slump-12-government-borrowing-june-figure-lowest-2019-horizon-business-live](https://www.theguardian.com/business/live/2024/jul/19/retail-sales-great-britain-slump-12-government-borrowing-june-figure-lowest-2019-horizon-business-live)

⁴ [hXXps://nasstatus.faa\[.\]gov/](https://nasstatus.faa[.]gov/)

⁵ [hXXps://www.reuters\[.\]com/technology/frontier-says-operations-impacted-by-microsoft-outage-2024-07-19/](https://www.reuters.com/technology/frontier-says-operations-impacted-by-microsoft-outage-2024-07-19/)

⁶ [hXXps://news.sky\[.\]com/story/mass-it-outage-hits-companies-around-the-world-as-planes-grounded-13180809](https://news.sky[.]com/story/mass-it-outage-hits-companies-around-the-world-as-planes-grounded-13180809)

⁷ [hXXps://supportportal.crowdstrike\[.\]com/s/login/?ec=302&startURL=%2Fs%2Fget-help](https://supportportal.crowdstrike[.]com/s/login/?ec=302&startURL=%2Fs%2Fget-help)

leave many organizations that remotely manage the hundreds—and even thousands—of Windows devices within their infrastructure without a remote, operational solution. Additionally, the aforementioned workaround likely needs to be deployed on all devices before security teams are able to implement any forthcoming security updates issued by the vendor.

While threat actor communities continue to discuss the ongoing incident, ZeroFox has identified no evidence of cyber threat actors claiming credit for the outage. However, ZeroFox notes that threat actors may seek to exploit the ongoing outages, including by:

- Taking advantage of stretched security infrastructure, performing attacks against targets that may otherwise draw quick attention and be identified.
- Leveraging the outage as a lure in social engineering attacks.
- Targeting high-profile victims that choose to remove their EDR suite in response to the outage, thereby leaving them vulnerable.

| Recommendations

- Where possible, deploy the vendor's recommended workarounds outlined in this report.
- Monitor for further workarounds and updates published by the vendor.
- Affected users should contact CrowdStrike through official channels.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%