Cyber Case Study Program

CrowdStrike Cyber-Case: Update to Global Outage

Case Number ACI-01-2026

Nick Dumitru

Editor in Chief: Karen Guttierri, PhD
Lead Editor: Volker Franke, PhD
Managing Editor: Anne Chance, PhD

About Case Studies

The ACI-TRENDS Global Cybersecurity Case Program is administered by the Army Cyber Institute at the United States Military Academy at West Point and publishes cybersecurity-related teaching cases, simulations and interactive exercises for use in academic and professional classrooms.

What are case studies?

Case studies are high-impact interactive learning tools structured around real or realistically simulated events placing learners in the role of decisionmakers confronting complex problems, tradeoffs, and uncertainty. Case studies immerse participants in the problem and its dilemmas.

Why use case studies?

Immersing participants cognitively and emotionally in this way requires them to grapple with ambiguity, incomplete information, and competing priorities while developing plausible courses of action.

Case studies are particularly important because cyber incidents unfold across technical, organizational, legal, and human domains simultaneously.

Case studies make invisible systems and cascading consequences visible, demonstrate how theory and policy apply under pressure, and build the analytical judgment required to anticipate, assess, and respond to real-world cyber threats.

Where to find ACI case study series.

More information on the case method can be found:

1. At the TRENDS Website: https://trendsglobal.org/whats-trending/
2. Decision-Making under Uncertainty: Using Case Studies for Teaching Strategy in Complex Envi-ronmentsby Volker Franke, PhD. https://jmss.org/article/view/57957

DISCLAIMER: Views expressed in this publication are those of the author and do not represent those of the Army Cyber Institute, West Point, the United States Army, TRENDS Global, or any government agency. This draft is developed for discussion purposes. Please check with the Army Cyber Institute or TRENDS Global before sharing or quoting.

About the Author

Nicusor Dumitru is an accomplished IT professional, educator, and cybersecurity specialist with expertise spanning security operations, systems administration, and higher education. He currently serves as a Lecturer of Computer Science at the University of North Georgia, teaching undergraduate courses in computer science and information systems to approximately 100 students per semester, while also contributing to the university's Cybersecurity Curriculum Development Committee.

Nicusor holds a Master of Science in Cybersecurity from Kennesaw State University, earned with a 4.0 GPA, and a Bachelor of Science in Cybersecurity from the University of North Georgia, graduating Summa Cum Laude. His technical work includes building a personal virtual Security Operations Center, leading threat modeling and penetration testing engagements, and co-developing a novel mobile security alarm published in IEEE Xplore. He holds a CompTIA Security+ certification and is proficient in a broad range of cybersecurity tools including Splunk, Wazuh, Metasploit, and Kali Linux.

A multilingual professional fluent in English and Romanian, Nicusor is committed to bridging the gap between technical cybersecurity practice and accessible, engaging education.

CrowdStrike Cyber-Case: Update to Global Outage

In February 2024, CrowdStrike introduced a new sensor capability to enable visibility into possible novel attack techniques that may abuse certain Windows mechanisms.

Updates are very important for the proper working of modern computer systems, as they provide up to date security, bug fixes and improved performance. Thus, they allow administrators to patch vulnerabilities, remove any issues with bugs and allow the software to be kept current.

On July 19, 2024, a massive IT outage took place due to the failure of a software update coming from CrowdStrike, one of the top global cybersecurity firms. The outage affected more than 8.5 million Windows devices and led to severe problems delivering services in domains ranging from airlines to hospitals.[1] CrowdStrike fixed the issue in less than a week, but it revealed serious issues with the automated updates used by IT infrastructure.

The Incident

In February 2024, CrowdStrike found that hackers compromised "named pipes", a mechanism used for communication between processes on Windows machines. The attackers could exploit these named pipes so that they would allow communication between malware installed on the victim machines and their command-and-control servers.[2]

On July 19, 2024, a Rapid Response Content update was delivered to certain Windows hosts, evolving the new capability first released in February 2024.

To fix this problem, CrowdStrike created a new configuration update for its Falcon sensor, which defended Windows systems against cyberattacks with the help of artificial intelligence. The update changed server's Channel File 291, a heuristic protection file, increasing its rapid-response capability and thus allowing it to detect when named pipes were used by malware. CrowdStrike created and tested new fields for this file's dataset, which was used to collect information about emerging types of attacks.[3]

This first change was released on March 5, 2024, after it was successfully tested using CrowdStrike's standard procedures. Three other updates were released between April 8, 2024, and April 24, 2024, without visible issues.[4] The last update was launched on July 19, 2024. Unfortunately, this update had an out-of-bounds error due to a coding mistake, resulting from the fact that the Falcon sensor could only receive 20 input fields, but the new update had 21 fields.[5]

1 Cunningham, A. (2024, July 24). CrowdStrike blames testing bugs for security update that took down 8.5M Windows PCs. ***Ars Technica***. https://arstechnica.com/information-technology/2024/07/crowdstrike-blames-testing-bugs-for-security-update-that-took-down-8-5m-windows-pcs/

2 Hay, L., Burgess, N.M., Greenberg, A. (2024, July 19). How one bad CrowdStrike update crashed the world's computers. ***Wired***. https://www.wired.com/story/crowdstrike-outage-update-windows/

3 CrowdStrike. (n.d.). Falcon content update: Remediation and guidance hub. Retrieved September 18, 2025, from https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

4 Coker, J. CrowdStrike reveals rapid response content update caused global outage. (2024, July 24). ***Infosecurity Magazine***. https://www.infosecurity-magazine.com/news/crowdstrike-response-update-outage/

5 Bott, E. What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer. (2024, July 24). ***ZDNet***. https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/

[6] As a result, the updated systems were trying to read memory outside the expected range, causing them to crash. [7] [8] Because of this error, the Falcon sensor and the systems containing it became inoperable and triggered the Blue Screen of Death (BSOD). [9] [10] Even worse, the systems were caught in a perpetual reboot loop and users found that they could not roll back the update or remove the file that caused the problem. [11]

The news outlets started to give details about the outage as early as July 19. For example, Reuters wrote that "***Cybersecurity firm CrowdStrike has deployed a fix for an issue that triggered a major tech outage […] disrupting operations at companies across multiple industries."*** [12]

The impact of the faulty update was increased by the way it was distributed. CrowdStrike's standard procedures for Falcon platform updates was to send updates to the endpoints as soon as they were ready. During this process, the policies that systems administrators usually put in place were ignored, because the updates were considered threat-detection data and not new software versions. Security specialist Patrick Wardle, the creator of the nonprofit Objective-See Foundation, noted that "***channel updates ...bypassed client's staging controls and was rolled out to everyone regardless […] as this was 'content' update (vs. a version update).***"[13]

This is what a pull-out will look like

After discovering the issue, CrowdStrike began to work on a solution, and suggested ways to revert the update. Unfortunately, their intervention was too late for 8.5 million Windows devices around the world, coming only after they had already applied the faulty update.[14] CrowdStrike officially revealed the cause of the outage on July 22, 2024. [15]

This event showed that, ironically, even though updates are created to improve

6 CrowdStrike. (2024, July 19). Falcon update for Windows hosts technical details. https://www.crowdstrike.com/en-us/blog/falcon-update-for-windows-hosts-technical-details/
7 CrowdStrike. (n.d.). Falcon content update: Remediation and guidance hub. Retrieved September 18, 2025, from https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/
8 Kerner, S. M. (2024, October 25). CrowdStrike outage explained: What caused it and what's next. ***TechTarget***. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next
9 Kerner, S. M. (2024, October 25). CrowdStrike outage explained: What caused it and what's next. T***echTarget***. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next
10 Hay, L., Burgess, N.M., Greenberg, A. (2024, July 19). How one bad CrowdStrike update crashed the world's computers. ***Wired***. https://www.wired.com/story/crowdstrike-outage-update-windows/.
11 Cunningham, A. Microsoft says 8.5M systems hit by CrowdStrike BSOD, releases USB recovery tool. (2024, July 22). ***Ars Technica***. https://arstechnica.com/information-technology/2024/07/microsoft-says-8-5m-systems-hit-by-crowdstrike-bsod-releases-usb-recovery-tool/
12 Siddiqui, Z. (2024, July 19). CrowdStrike deploys fix for issue causing global tech outage. ***Reuters***. https://www.reuters.com/technology/crowdstrike-says-actively-working-with-customers-impacted-by-outage-2024-07-19/
13 Wardle, P. (2024, July 19). Note "channel updates ...bypassed [Post]. X. [@patrickwardle]. https://x.com/patrickwardle/status/1814367918425079934
14 Greenberg, A. (2024, July 19). CrowdStrike Fault Causes Global IT Outages. ***Infosecurity Magazine***. https://www.infosecurity-magazine.com/news/crowdstrike-fault-it-outages/
15 Bott, E. What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer. (2024, July 24). ***ZDNet***. https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/

system security and stability, they can sometimes have the opposite effect, weakening the systems instead.

The Aftermath

By July 22, 2024, CrowdStrike and Microsoft recommended procedures that could be used by their users to fix the problem. The main solution was to restart the affected machines multiple times and then roll back the update before they crashed again. Most of the systems affected by the outage were restored using this solution, although some clients had to ***"reboot as many as 15 times to give computers a chance to download the update."***[16] But not all systems could be fixed this way. Since many computers never stopped crashing, their administrators had to remove the faulty system file manually before they could restart the computers and fix the update. [17] [18]

For systems where that method hasn't worked—and Microsoft has recommended customers reboot as many as 15 times to give computers a chance to download the update the recommended fix has been to delete the bad .sys file manually.

Microsoft also released tools to help users recover. These tools automated some parts of the recovery process, like using USB recovery devices or the Preboot Execution Environment (PXE). However, this method of rebooting did not work on systems which had their external booting disabled by their administrators for security reasons. [19]

Many people whose computers crashed, such as this user from X, were not happy with the solution offered by CrowdStrike: "I***t's been almost another 24hrs and we are still no closer to answers from @CrowdStrike, in fact the open source community of engineers on X has delivered more insights and actionable items than the entirety of CrowdStrike's turn it off, turn it on again 15 times boot loop 'fix'.***" [20]

The Effects

The effects of the outage lasted longer. System crashes spread throughout the entire world immediately after the update and disrupted services, including critical ones. Describing the problems, The Verge wrote that "***thousands of Windows machines are experiencing a Blue Screen of Death (BSOD) issue at boot today, impacting banks, airlines, TV broadcasters, supermarkets, and many more businesses worldwide."***[21] The banks, airlines, and television stations in Australia went offline. Similarly, business and media organizations from Europe were affected. Sky News' morning show from the United Kingdom, was out. They broadcast instead of their normal program, an apology message to

16 Cunningham, A. Microsoft says 8.5M systems hit by CrowdStrike BSOD, releases USB recovery tool. (2024, July 22). ***Ars Technica***. https://arstechnica.com/information-technology/2024/07/microsoft-says-8-5m-systems-hit-by-crowdstrike-bsod-releases-usb-recovery-tool/

17 Cunningham, A. Microsoft says 8.5M systems hit by CrowdStrike BSOD, releases USB recovery tool. (2024, July 22). ***Ars Technica***. Ibidem.

18 Atkinson, R. (2024, July 22). Buggy CrowdStrike EDR update crashes Windows systems worldwide. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/crowdstrike-outage

19 Cunningham, A. Microsoft says 8.5M systems hit by CrowdStrike BSOD, releases USB recovery tool. (2024, July 22). ***Ars Technica***. Ibidem.

20 Jacob, A. It's been almost another 24hrs and we are still no closer to answers from @CrowdStrike. (2024, July 20). https://x.com/MickeySteamboat/status/1814764919406874855?referrer=grok-com

21 Warren, T. Major Windows BSOD issue hits banks, airlines, and TV broadcasters. (2024, July 19). ***The Verge***. https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue

their viewers from a mobile phone. [22] [23]

Airlines from all over the world, such as Ryanair, Delta, United, and American Airlines were also affected. Airports were not spared from this problem, even reverting to handwritten boarding passes as one airport in India did. [24] The Berlin Airport in Germany had technical issues which made them delay or cancel flights. Because around the world thousands of flights were canceled or delayed, many airline staff and passengers were stranded at airports. [25] Their frustration can be seen from an online message of a X user: "***Everything is broken thanks to the CrowdStrike virus. Crew scheduling is absolutely overwhelmed. My wife is a flight attendant and is sleeping in the lounge after working a 12-hour day and can't get home or find a hotel room and her flight is cancelled***." [26]

Hospitals in the US reported problems on Friday morning with their IT systems, affecting many patients.

United States 911 emergency services in states such as Alaska, Minnesota, Arizona, Indiana, Ohio, and New Hampshire were affected too. [27] [28] Even worse, many healthcare providers could not offer care to their patients. Hospitals in the US and the UK, such as the Massachusetts General Hospital and Mass General Brigham were affected and were struggling. As a result, they canceled non-urgent medical appointments and procedures. Pharmacies had to close during the outage because it made it impossible for them to accept payments. [29] A nurse at GBMC HealthCare in Maryland posted on X about the problems they had: "***Our hospital is fully down due to #Crowdstrike issue. No phones, no computers [...] It's an all hands on-deck kind of day. I hope our patients remain safe***."[30]

Even more, the world's finances have lost a lot of money. Analysts, such as those from the consulting firm Parametrix, estimated that the impact on the Fortune 500 companies reached $5.4 billion, even after excluding Microsoft. Twenty-five percent of these businesses were affected. Healthcare and banking took most of these losses, with $1.94 billion, followed by banking, with $1.15 billion. Because almost all airline companies in the world were affected, they lost an estimated

"The volume is likely to reach $5.4 billion in costs for Fortune 500 companies, according to a report from Parametrix. Parametrix researchers have found that roughly 25% of Fortune 500 companies experienced disruptions due to the incident, the most heavily affected industries financially being healthcare ($1.94 billion in estimated losses) and banking ($1.15 billion).

22 Warren, T. Major Windows BSOD issue hits banks, airlines, and TV broadcasters. (2024, July 19). ***The Verge***. https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue
23 Collins. K. Microsoft-CrowdStrike outage causes chaos for flights, hospitals, and businesses globally. (2024, July 19). ***CNET***. https://www.cnet.com/tech/services-and-software/microsoft-crowdstrike-outage-causes-chaos-for-flights-hospitals-and-businesses-globally/
24 Warren, T. Major Windows BSOD issue hits banks, airlines, and TV broadcasters. (2024, July 19). ***The Verge***. https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue
25 Collins. K. Microsoft-CrowdStrike outage causes chaos for flights, hospitals, and businesses globally. (2024, July 19). ***CNET***. https://www.cnet.com/tech/services-and-software/microsoft-crowdstrike-outage-causes-chaos-for-flights-hospitals-and-businesses-globally/
26 Royce, T. [@TomRoyce]. (2024, July 22). Deep breathe. Everything is broken thanks to the CrowdStrike virus [Post]. X. https://x.com/TomRoyce/status/1815229448041414825
27 Collins. K. Microsoft-CrowdStrike outage causes chaos for flights, hospitals, and businesses globally. (2024, July 19). ***CNET***. https://www.cnet.com/tech/services-and-software/microsoft-crowdstrike-outage-causes-chaos-for-flights-hospitals-and-businesses-globally/
28 Warren, T. Major Windows BSOD issue hits banks, airlines, and TV broadcasters. (2024, July 19). ***The Verge***. https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue
29 Collins. K. Microsoft-CrowdStrike outage causes chaos for flights, hospitals, and businesses globally. (2024, July 19). ***CNET***. https://www.cnet.com/tech/services-and-software/microsoft-crowdstrike-outage-causes-chaos-for-flights-hospitals-and-businesses-globally/
30 Chandler, D. [@nursedanakay]. (2024, July 19). Our hospital is fully down due to #Crowdstrike issue. No phones, no computers, no safety [Post]. X. https://x.com/nursedanakay/status/1814260635414237649

$0.86 billion.[31]

Finally, chaos followed in the aftermath due to the spread of rumors about cyberattacks on social media, although CrowdStrike's CEO George Kurtz clarified that it was not a cybersecurity incident.[32] However, opportunistic attacks did take place, since hackers were using the outage as a window of opportunity to launch phishing campaigns.[33] Infosecurity Magazine gave examples of such attacks: "***Cybercriminals have been identified sending phishing emails purporting to be CrowdStrike support and impersonating CrowdStrike staff in phone calls.***" Hackers also created scams that involved the use of malicious ZIP files pretending to hold a fix for the issue but instead were deploying Trojan malware. [34]

Final thoughts

The CrowdStrike 2024 outage showed how the catastrophic failure of a single software update can result in the crash of millions of Windows devices. It underlined the vulnerability of IT infrastructure, causing massive damage to dozens of business areas and leading to financial losses of billions. Unfortunately, such outages are not unique; they have happened before and are likely to happen again. To address this challenge, we need first to determine the dilemmas raised by this case and to find solutions to resolve them. What trade-offs should we consider, and what can we do to avoid disruptions in the future born from vulnerabilities in automated IT infrastructure updates?

31 CrowdStrike outage losses estimated at a staggering $5.4B. (2024, July 26). ***Dark Reading***. https://www.darkreading.com/cybersecurity-operations/crowdstrike-outage-losses-estimated-staggering-54b
32 Silberling, A. (2024, July 19). From the Sphere to false cyberattack claims, misinformation runs rampant amid CrowdStrike outage. ***TechCrunch***. https://techcrunch.com/2024/07/19/from-the-sphere-to-false-cyberattack-claims-misinformation-runs-rampant-amid-crowdstrike-outage/
33 Coker, J. Cybercriminals exploit CrowdStrike outage chaos. (2024, July 22). ***Infosecurity Magazine.*** https://www.infosecurity-magazine.com/news/cybercriminals-exploit-crowdstrike/
34 Coker, J. Cybercriminals exploit CrowdStrike outage chaos. (2024, July 22). ***Infosecurity Magazine.*** https://www.infosecurity-magazine.com/news/cybercriminals-exploit-crowdstrike/