Congressional Research Service
Informing the legislative debate since 1914

IT Disruptions from CrowdStrike's Update: Frequently Asked Questions

July 24, 2024

Congressional Research Service
https://crsreports.congress.gov
R48135

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

IT Disruptions from CrowdStrike's Update: Frequently Asked Questions

The use of information technology (IT) across industries has created opportunities for disruptions and vulnerabilities in the supply chain for products and services. The impact of these disruptions may be more widespread when components of IT systems are concentrated among a limited number of providers.

On July 19, 2024, CrowdStrike, a cybersecurity firm that delivers its products and services via a cloud computing platform, released a software update with a defective file for devices using the Windows operating system, causing some Windows devices to crash. Based on reporting from various news agencies, the faulty update affected entities around the world, including airlines, banks, retailers, and emergency service providers. As of July 20, 2024, Microsoft estimates that about 8.5 million Windows devices, or less than 1% of all Windows devices, were affected by CrowdStrike's faulty update.

SUMMARY

R48135

July 24, 2024

Clare Y. Cho, Coordinator
Specialist in Industrial Organization and Business Policy

Brian E. Humphreys
Analyst in Science and Technology Policy

Rachel Y. Tang
Analyst in Transportation and Industry

Paul Tierno
Analyst in Financial Economics

Ling Zhu
Analyst in Telecommunications Policy

Contents

Tables

Contacts

The use of information technology (IT) across industries has created opportunities for disruptions and vulnerabilities in the supply chain for products and services. For example, some firms may be more susceptible to system failures, data breaches, and cyberattacks than others depending on the security of the IT systems used.[1] Recent examples include the February 2024 cyberattack on Change Healthcare, a subsidiary of UnitedHealth Group, Inc.,[2] and a series of data breaches beginning in April 2024 that may have affected about 165 organizations using Snowflake, a cloud-based data management platform.[3] The impact of these disruptions may be more widespread when components of IT systems are concentrated among a limited number of providers.

On July 19, 2024, CrowdStrike Holdings, Inc. (hereinafter CrowdStrike) released a software update with a defective file for devices using the Windows operating system, causing some Windows devices to crash. CrowdStrike and Microsoft subsequently released updated safe files and recovery tools.[4] Some users were able to fix the issue by rebooting impacted devices multiple times, while others had to take additional steps.[5] CrowdStrike's faulty update does not appear to be related to a cyberattack or data breach; instead, it is an example of the pervasiveness of some IT components and how an issue with an IT component may affect multiple sectors simultaneously, resulting in a host of disruptions domestically and internationally.

This FAQ provides a description of CrowdStrike and the faulty update and discusses how the faulty update affected certain sectors in the United States. For an overview of the incident and potential considerations for Congress, see CRS Insight IN12392, *The July 19th Global IT Outages*, by Chris Jaikaran.

How did the faulty CrowdStrike update occur, and what is CrowdStrike?[6]

CrowdStrike delivers cybersecurity products and services to its customers via a cloud computing platform—the Falcon platform.[7] CrowdStrike, through its cloud-based platform, deploys and installs a software called the Falcon Agent or the Falcon Sensor on each connected endpoint device (e.g., individual computer) of its customers.[8] On July 19, 2024, CrowdStrike released "a

[1] For information on cyberattacks, see CRS Report R46974, *Cybersecurity: Selected Cyberattacks, 2012-2022*, by Chris Jaikaran; and CRS In Focus IF10559, *Cybersecurity: A Primer*, by Chris Jaikaran.

[2] CRS Insight IN12330, *The Change Healthcare Cyberattack and Response Considerations for Policymakers*, by Chris Jaikaran.

[3] Mandiant, "UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion," Google Cloud Blog, June 10, 2024, https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

[4] Intune Support Team, "New Recovery Tool to Help with CrowdStrike Issue Impacting Windows Endpoints," Microsoft Tech Community, July 20, 2024, https://techcommunity.microsoft.com/t5/intune-customer-success/new-recovery-tool-to-help-with-crowdstrike-issue-impacting/ba-p/4196959; and CrowdStrike, "Remediation and Guidance Hub: Falcon Content Update for Windows Hosts," last updated July 22, 2024, https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.

[5] Tom Warren, "Microsoft Releases Recovery Tool to Help Repair Windows Machines Hit by CrowdStrike Issue," *The Verge*, July 21, 2024, https://www.theverge.com/2024/7/21/24202883/microsoft-recovery-tool-windows-crowdstrike-issue-it-admins.

[6] Ling Zhu authored this section.

[7] CrowdStrike, SEC Form 10-Q: Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Quarterly Period Ended April 30, 2024, June 5, 2024, p. 28, https://ir.crowdstrike.com/static-files/6fd7c643-827b-4632-9cf3-790913da29a9.

[8] CrowdStrike, *SEC Form 10-K: Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934* (continued...)

sensor configuration update" over the cloud to its customers' endpoint computers that were running the Falcon sensor for Windows operating systems.[9] The update "triggered a logic error resulting in a system crash and blue screen [error]" on impacted computers.[10] Those computers that were online and downloaded the faulty update within a certain time period on that day "were susceptible to a system crash."[11] CrowdStrike's faulty update does not appear to be related to a cyberattack or data breach. The outage occurred as part of the company's effort to deliver its cybersecurity services.

CrowdStrike claims that its cybersecurity products through the Falcon Agent can identify and prevent "known and unknown malware and fileless attacks" to protect its customers' endpoint devices while "capturing and recording … endpoint data."[12] The cyberattack events and data captured by the agent are streamed back to the Falcon platform's cloud infrastructure in real time "in order to be further analyzed" to optimize its cybersecurity algorithms.[13] The agent can also be remotely reconfigured in real time to take other actions "as risk and threat postures change."[14] This agent is built to support major computer operating systems, including Microsoft's Windows.[15]

What Is Cloud Computing?

Cloud computing is a computer networking model that allows end users to remotely access a shared pool of computing resources, such as computer servers, data storage devices, networks, software, and computer applications and services. In this model, end users do not need to acquire, install, deploy, manage, maintain, or perform their own updates of related hardware, software, data, networks, and services on their local computer systems. A cloud computing service provider delivers these computing resources, capabilities, and services virtually to end users on demand, mostly over internet-based networks.

A basic cloud computing service example is a web-based email service, in which users log into their online accounts to receive, compose, send, store, and organize emails. All functions are delivered to the user from the email service provider's server via the internet. Even if the user uses a different computer device, the user can still access the same online email service, so long as the user has internet access.

Cloud computing is a model for many IT companies to deliver their products and services. It has also become a common IT option adopted by many public and private organizations.

What businesses were affected by CrowdStrike's faulty update?[16]

As of July 20, 2024, Microsoft estimates that about 8.5 million Windows devices, or less than 1% of all Windows devices, were affected by CrowdStrike's faulty update.[17] The faulty update

for the Fiscal Year Ended January 31, 2024, March 7, 2024, p. 13, https://ir.crowdstrike.com/static-files/29e71f45-3c39-4c2c-9159-5e7bb9f3315b (hereinafter CrowdStrike, *SEC Form 10-K*). Although the company called the software "the Falcon Agent" in its SEC filings, the company also uses the term "the Falcon sensor" to refer to the same software when explaining the technology on its website. See Crowdstrike, "What is CrowdStrike? Falcon Platform FAQ: 'Deployment,'" accessed July 23, 2024, https://www.crowdstrike.com/products/faq/.

[9] CrowdStrike, "Technical Details: Falcon Content Update for Windows Hosts," blog post, July 20, 2024, https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/.

[10] Ibid.

[11] Ibid.

[12] CrowdStrike, *SEC Form 10-K*, p. 13.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Clare Cho authored this section.

[17] David Weston, "Helping Our Customers Through the CrowdStrike Outage," Microsoft Blog, July 20, 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

affected various entities around the world, including airlines, banks, retailers, and emergency service providers.[18] On its website, CrowdStrike states that its software is used by 298 of the Fortune 500 companies, including food and beverages companies, automotive companies, manufacturers, health care providers, and firms providing financial services.[19]

How did CrowdStrike's faulty update affect airlines?[20]

CrowdStrike's faulty update had a significant effect on some airlines. On July 19, 2024, and the following weekend, Delta Airlines, American Airlines, United Airlines, Allegiant Air, and Spirit Airlines grounded flights in the United States, which led to thousands of flight cancellations, extensive delays, and long waits at airports.[21] While most airlines appeared to have recovered from the disruptions and restored operations after the weekend, issues at Delta persisted beyond the initial incident weekend.[22] Delta reportedly has canceled more than 5,500 flights since the start of the Friday outage, including at least 700 flights on July 22, accounting for about two-thirds of all cancellations worldwide that day.[23]

The Office of Aviation Consumer Protection in the U.S. Department of Transportation reportedly released a statement on Tuesday, July 23, 2024, that it was launching an investigation into Delta's widespread flight disruptions and concerning customer service failures.[24]

How did CrowdStrike's faulty update affect banks?[25]

Several banks reported being affected by CrowdStrike's faulty update, according to various media reports.[26] Some of the banks that experienced issues include TD Bank, Bank of America, JP Morgan Chase, Wells Fargo, Synovus Financial, Fifth Third Bank, Canandaigua National Bank, and American Express.[27]

---

[18] For example, see Alexander Smith and Kevin Collier, "What We Know About the Global Microsoft Outage," *NBC News*, July 19, 2024, https://www.nbcnews.com/tech/tech-news/microsoft-outage-crowdstrike-global-airlines-windows-fix-rcna162685; and Rebecca Schneid, "CrowdStrike's Role in the Microsoft IT Outage, Explained," *Time*, last updated July 20, 2024, https://time.com/7000476/microsoft-it-outage-crowdstrike-role-what-happened-explanation/.

[19] CrowdStrike, "About CrowdStrike," https://www.crowdstrike.com/about-us/.

[20] Rachel Tang authored this section.

[21] David Koenig, "Your Flight Was Canceled by the Technology Outage. What Do You Do Next?," Associated Press, last updated July 19, 2024, https://apnews.com/article/outage-airlines-flights-canceled-crowdstrike-microsoft-044954aada0fa4f95c0119233c6316a6.

[22] David Koenig, "Most Airlines Except One Are Recovering from the CrowdStrike Tech Outage. The Feds Have Noticed," Associated Press, July 22, 2024, https://apnews.com/article/outage-airline-delta-40fc208ac838cafab40482b731072018.

[23] Ibid.

[24] Tara Suter, "Feds Launch Investigation Into Delta After Flight Fiasco," July 23, 2024, *The Hill*, https://thehill.com/policy/transportation/4787799-dot-investigation-delta-flight-cancellations/.

[25] Paul Tierno authored this section.

[26] For example, see Carter Pape and Miriam Cross, "Tech Issues Afflict Banks, Microsoft After Critical CrowdStrike Glitch," *American Banker*, July 19, 2024, https://www.americanbanker.com/news/bank-customers-report-tech-issues-amid-crowdstrike-microsoft-problems; and PYMNTS, "CrowdStrike Aftermath: Five Things You Need to Know," July 22, 2024, https://www.pymnts.com/connectedeconomy/2024/crowdstrike-aftermath-five-things-you-need-to-know/.

[27] Carter Pape and Miriam Cross, "Tech Issues Afflict Banks, Microsoft After Critical CrowdStrike Glitch," *American Banker*, July 19, 2024, https://www.americanbanker.com/news/bank-customers-report-tech-issues-amid-crowdstrike-microsoft-problems.

The types of problems reported differ across affected banks. They include temporary difficulties processing transactions, inability of customers to access accounts, and trouble among employees logging onto their workstations.

What role did the Cybersecurity and Infrastructure Security Agency (CISA) and relevant Sector Risk Management Agencies (SRMAs) play in consequence mitigation and recovery of critical infrastructure functions related to CrowdStrike's faulty update?[28]

There are currently 16 federally designated critical infrastructure sectors, which cover wide areas of the national economy, governance, and essential services.[29] In each critical infrastructure sector, one or more federal agencies fulfils the role of SRMA.[30] These federal agencies coordinate risk management activities in their respective sectors and lead federal outreach to owners and operators of critical infrastructure systems and assets in these sectors. Infrastructure owners and operators within several sectors were affected by the outage. **Table 1** lists critical infrastructure sectors that were affected by CrowdStrike's faulty update and corresponding SRMAs.

Table 1. Sector Risk Management Agencies for Critical Infrastructure Sectors Affected by CrowdStrike's Faulty Update

Critical Infrastructure Sector	Sector Risk Management Agency
Emergency Services	CISA
Government Services	CISA and GSA
Healthcare and Public Health	HHS
Transportation	DHS (TSA, USCG) and DOT

Source: Cybersecurity and Infrastructure Security Agency (CISA); and CRS analysis of publicly available reports.

Notes: DHS = Department of Homeland Security; DOT = Department of Transportation; GSA = U.S. General Services Administration; HHS = Department of Health and Human Services; TSA = Transportation Security Administration; USCG = U.S. Coast Guard.

CISA created a web-based resource providing updates and links to information on the outage, referring users to CrowdStrike resources for affected entities.[31]

[28] Brian Humphreys authored this section.

[29] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[30] The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, NSM-22, April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

[31] CISA, "Widespread IT Outage Due to CrowdStrike Update," https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

Author Information

Clare Y. Cho, Coordinator
Specialist in Industrial Organization and Business Policy

Brian E. Humphreys
Analyst in Science and Technology Policy

Rachel Y. Tang
Analyst in Transportation and Industry

Paul Tierno
Analyst in Financial Economics

Ling Zhu
Analyst in Telecommunications Policy

Disclaimer