Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

The July 19th Global IT Outages

July 23, 2024

On July 19, 2024, cybersecurity firm CrowdStrike pushed an update to its software that caused some devices running the Windows operating system to crash. The day before, there was a separate outage of Microsoft Azure cloud services. The widespread adoption of both Microsoft products and CrowdStrike's cybersecurity services led to global disruptions to industries like aviation, emergency services, financial services, healthcare, and retail. This CRS Insight discusses these events, their impacts, and potential considerations for Congress.

Event

CrowdStrike runs an endpoint detection and response platform—Falcon. Falcon includes an application on the host device (e.g., a computer) along with cloud services to detect potentially anomalous activity on the device, analyze activity on it for threats, and report suspicious events to information technology (IT) administrators. It also automates certain mitigation activities for the potential risk. On July 19, CrowdStrike issued an update to host devices with a Falcon sensor. The update included a defective file for Windows machines that caused receiving systems to display an error screen and lock users out of their devices. Microsoft estimates that this event affected 8.5 million systems, which is less than 1% of total Windows machines. Linux and Mac hosts were not affected.

Separately, on July 18, 2024, Microsoft experienced a disruptive incident with its Azure cloud services. In this event, virtual machines (VM) became inaccessible to cloud subscribers because of an error in the way Microsoft allows access to those machines as well as an infrastructure failure. Corporate customers who rely on Azure were unable to access their services hosted on Azure in the Central United States region during this event, which lasted about a half-day.

As the software development lifecycle evolved, companies moved to a continuous update delivery model and built distribution channels right into their services—removing friction in updating their products, but also expediting adverse effects when there are issues with those updates (like with the SolarWinds incident).

In both instances, administrators were able to rapidly diagnose the issues and push corrections out to affected systems. For the CrowdStrike incident, most customers were able to reboot their devices and have a safe update pulled to their systems and automatically install to restore operations. Some users had

CRS INSIGHT
Prepared for Members and
Committees of Congress

to manually delete the bad file and apply the update. For the Azure incident, Microsoft corrected the error and no action was necessary on the part of the user.

To date, the companies have said that these incidents were not cyberattacks, but rather software glitches. Customer data and the protections the software provides do not appear to have been compromised during the events.

Impacts

The IT services at play in both of these incidents (i.e., Falcon and Azure) are predominantly used by business customers globally. As the update was pushed out, business users had difficulty accessing their computing devices.

Some of the reported impacts from the July incidents include:

- Airlines had to delay or cancel flights.
- Live news broadcasts were delayed.
- Emergency alert systems and 911 centers were unable to function.
- Bankers could not process trades.
- Hospitals could not honor appointments.

These effects did not impact every company in an industry, or every location globally. They were felt sporadically across industries around the world, and the sudden onset compounded challenges.

Considerations for Congress

Given the wide scale and short order of these events, policymakers may choose to investigate the root cause of each incident and the nature and speed of agency responses, and may consider policies to reduce impacts in the future. Some areas of potential focus include:

- **Critical Infrastructure Resiliency**—The federal government has long been concerned with the *security* of industries that are vital to the United States economy. But a growing area of interest is the *resilience* of those industries, regardless of the risks they face. Although the Falcon and Azure outages were not caused by security incidents, they did become national security events that underscore the importance of business continuity plans and the ability to overcome disruptions.
- **Role of Regulators**—These outages affected business customers directly; however, the customers of those businesses bore much of the burden. Congress may choose to consider the role of regulators in addressing hardships felt by individuals during events such as these.
- **Social Media**—As the CrowdStrike outage spread, so did information about it on social media. One trend was for parody accounts to mock that they were a new employee pushing out their first update. Automated systems at some social media companies collected this information as being related to the incident and promoted it in feeds. Congress may choose to explore the role of automation in filtering and promoting social media content, especially as it relates to fast-breaking news events for which there may be national security implications.
- **Vendor Dominance**—Windows is by far the most popular desktop operating system worldwide with over 70% market share. CrowdStrike maintains nearly a fifth of endpoint security product market share. These outages highlight the risks related to market

- domination by a few providers and reliance on cloud-services. Incidents at a single company (particularly at ones providing essential services, or internet infrastructure) could have outsized impact on individual and corporate customers as these companies become more intertwined and dependent on each other.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.