CrowdStrike Software bug

Emmett Kjolseth

Washington State University

CPTS 322: Software Engineering I

Dr. Parteek Kumar

January 17, 2025

The CrowdStrike software bug incident took place on July 19, 2024. The cybersecurity firm CrowdStrike released a faulty update to its Falcon security software, which led to a global IT outage affecting an estimated 8.5 million computers across the globe (Investors Business Daily, 2024). The role of CrowdStrike as a cybersecurity firm was to build what's called Endpoint Detection and Response (EDR). EDR is a software that runs continuously on every workstation in a company and checks for behavior that indicates the computer has been infected with a virus. This Since Microsoft relies on CrowdStrike as a third-party for security solutions, computers with window operating systems ended up getting the "Blue Screen of Death" crashing millions of computers.

The CrowdStrike software bug was a flaw during an update. The bug caused an out-of-bound error which led the windows systems to crash. This bug also ended up having a large impact on the aviation sector. Delta Airlines had the worst impact, canceling more than 6,000 flights in 5 days, disrupting around 1.3 million customers, and costing at least

500 million dollars (Investors Business Daily, 2024). Other airlines and air traffic control communications were affected and all these problems caused ripple effects as well. Since scheduling for flights was thrown off, it threw off other interconnected flights as well, causing more delays.

Having less reliance on third parties for things like cybersecurity could be a useful strategy to prevent issues like this in the future. The CrowdStrike incident was due to an error caused by them, but it also pointed out issues with companies like Microsoft relying on third parties for cybersecurity. According to Stanford news, “This incident serves as a stark reminder of just how reliant we have become on incredibly complex software systems and the large number of dependencies that each system has.” (Stanford News, 2024). The problem with systems being dependent on one another arises because the third parties have kernel-level access, which is necessary to detect malware in computers. This reliance means that any problems with third party applications can cascade into larger system failures as well, which is why this bug crashed window systems. If a company relies on a third party for their products, then there should be extra measures in place to make sure updates won’t cause cascading effects. The causes of the CrowdStrike bug highlight the importance of quality assurance in software development.

The CrowdStrike software bug in 2024 was a huge disaster and cost a lot of money and time. From reading about the incident, it seems clear that this issue isn’t expected to be the only one because of how reliant we are on complex and interconnected software systems. To reduce the risk of similar incidents, companies should consider reducing their reliance on third party systems and focus on internal systems for their products that are heavily relied on.

Investors Business Daily. (2024). *CrowdStrike faces corporate crisis after security software glitch*. Retrieved from https://www.investors.com/news/technology/crowdstrike-stock-crwd-cybersecurity-corporate-crisis-management/?utm_source=chatgpt.com

Stanford News. (2024, July). *An expert's overview of the CrowdStrike outage*. Stanford News. Retrieved from https://news.stanford.edu/stories/2024/07/an-expert-s-overview-of-the-crowdstrike-outage