CrowdStrike Bug Analysis and Preventative Measures for the Future

Collin Bale

Computer Science, Washington State University

CPT_S 322

Dr. Parteek Kumar

January 1, 2025

CrowdStrike, a company who advertises “Setting the standard for security in the cloud era”, experienced a major outage on July 19th, 2024. This outage, caused by a bug in an update released that morning, crashed roughly 8.5 million systems with no way of effectively restarting them. This one faulty update resulted in what CNN estimated to be north of “$5 billion in direct losses”. The CrowdStrike Falcon software is effectively an antivirus software, however it differs the general public’s understanding of software and applications. CrowdStrike Falcon is an enterprise level software that runs side by side with the Windows OS. This means that this software has full access to the entire machine it runs on. This enables Falcon to more effectively detect and remove viruses, ransomware, and any other form of known virus.

Due to the nature of CrowdStrike Falcon and Microsoft Windows OS, the recovery process for affected computers is not as simple as removing the faulty file delivered in the update. A result of the computer being unable to restart is that files are inaccessible, and Windows must be manually booted into “safe mode”. This process takes much longer to do and with limited IT members available at each company, as well as the sheer number of affected computers, this process led to a much lengthier response time when fully repairing this problem.

The aviation sector was heavily affected by this outage as it primarily hit their reservation and scheduling systems. Aviation as a whole requires near-seamless communication from end-to-end, and this bug put a significant part of that process to a screeching halt. By preventing this step of reservation and scheduling, the company was unable to do client-company transactions, as well as then take those transactions and effectively plan what planes are flying in and out, in addition to scheduling the gates and terminals associated with those flights. A major company affected by this bug was Delta. Delta has gone on record saying that an upwards of fifty percent of their company’s systems runs on Windows. Delta took significantly longer to return to doing business as usual, however knowing the process behind resetting the OS, this makes sense.

Preventing this issue in the future of course falls on CrowdStrike directly with better management and unit testing of update deployment. However, the public also needs to understand their role in preventing major outages like this. The primary preventative measure for most, if not all companies, should have been backups. Backups are important to both the security of a company’s data, but also the security of the systems that work with that data. Both elements are clearly important to a company’s success in properly doing their business and without proper backups, these elements are vulnerable to getting lost to data corruption, or severe delays as seen in this CrowdStrike incident.

CrowdStrike as a company will have to improve their quality assurance moving forward. A company as large as CrowdStrike, servicing as many enterprises as they are, has little to no room for error on this level. Code testing practices will also have to improve. Unit testing in code is extremely important in identifying and fixing potential bugs and vulnerabilities in programs. Quality assurance will help to stop bugs like this going forward and hopefully help the public to realize the vulnerable nature of their data and systems we all rely so heavily on as to avoid this situation taking place on this scale again in the future.

Works Cited

Fung, B. (2024, July 24). *We finally know what caused the global tech outage - and how much it cost | CNN business*. CNN. https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html

Kubota, T. (n.d.). *A computer scientist's take on the crowdstrike crash*. Stanford Report. https://news.stanford.edu/stories/2024/07/an-expert-s-overview-of-the-crowdstrike-outage

Wichter, Z. (2024, July 19). *Airlines rely on complex systems: Why The crowdstrike hiccup could cause days of chaos*. USA Today. https://www.usatoday.com/story/travel/airline-news/2024/07/19/airline-tech-glitch-flight-chaos/74471167007/