Jason Su

Cpts 322

CrowdStrike Bug

On July 11, 2024, widespread crashes occurred in Microsoft Windows around the world after an automatic update to CrowdStrike's Falcon cybersecurity software occurred. CrowdStrike, founded in 2011, is a major cybersecurity company, employing over 8000 people and making $300 billion per year (Scroxton, 2024). Falcon is a product of CrowdStrike that is used to stop cyberattacks and updates to the software, which are used to help identify new threats and improve the sensor, are delivered by cloud (Scroxton, 2024).

The bug occurred do to updates to a sensor configuration for Microsoft Windows that caused changes to configuration files, called Channel Files, specifically Channel File 291, that resulted in a logic error which caused Window systems to crash (CrowdStrike). About 8.5 million Windows machines were affected, although only making up less than one percent of all Windows devices (Cybersecurity and Infrastructure Security Agency [CISA], 2024), was enough to affect many different organizations around the world. Airlines like American Airlines, Delta, and Lufthansa, and financial, media, and healthcare organizations were reported being affected by the outages (Scroxton, 2024). More than 4000 flights were reported canceled within hours of the first outages (Burgess, 2024). While the problem was not caused by malicious actors, the Cybersecurity and Infrastructure Security Agency reported many actors taking advantage of the outages for malicious activity, including phishing scams and distributing malicious files (Cybersecurity and Infrastructure Security Agency [CISA], 2024).

The CrowdStrike bug shows that many software developers, especially those who make software that is widely use and used in important or essential parts of life, such as in travel, health, or the economy, need to make sure that bugs that could cause major issues are either avoided or caught and fixed before being officially updated, especially with cloud updates allowing companies to instantly update their software and immediately affect all services that use their software. This means companies or any group that develops software need to make improvements in testing and quality assurance of software. This may mean spending more time and having more people check the code and test how the software behaves before officially releasing the software or update. While testing software like this should be standard, according to Scientific America "…for some routine products like security tools, that may not happen" (Forno, 2024). This means efforts should be made for testing to be mandatory for upgrades in all cases, including for routine products where it was not mandatory before. In cases where an update to software is done by cloud, resulting in instant updates that a hard to fix or reverse, testing these updates in a controlled environment to see if any bugs occur before the program is released into the "wild" could be implemented to prevent events like this from occurring in the future.

This incident show how important testing software is and should be considered a wake-up call to software developers to make sure major bugs do not occur that would end up causing a major disrupting impact to many important components of our interconnected world. We can learn from this to improve how we test for bugs in software and also be more aware of the impact software has on our lives. We rely so much on our computers and software working correctly and the results of something going wrong with them can be far-reaching and costly. If we do not learn from this incident and make major changes to how we develop and test software, then incidents like this could easily happen again.

APA Citations

1. Cybersecurity and Infrastructure Security Agency. (2024, July 19). *Widespread IT outage due to CrowdStrike update*. U.S. Department of Homeland Security. Retrieved from

https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update

2. Forno, Richard. (2024, July 22). *Massive CrowdStrike tech outage highlights global vulnerabilities*. Scientific American. Retrieved from https://www.scientificamerican.com/article/massive-crowdstrike-tech-outage-highlights-global-vulnerabilities/

3. Scroxton, Alex (2024, July 29). *CrowdStrike update chaos explained: What you need to know*. Computer Weekly. Retrieved from https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know

4. Burgess, Matt. (2024, July 19). *Microsoft Windows outage: CrowdStrike and global IT problems*. Wired. Retrieved from https://www.wired.com/story/microsoft-windows-outage-crowdstrike-global-it-probems/

5. CrowdStrike. (2024, July 20). *Falcon update for Windows hosts: Technical details*. Retrieved from https://www.crowdstrike.com/en-us/blog/falcon-update-for-windows-hosts-technical-details/