**CrowdStrike Software Incident**

The CrowdStrike software incident impacted millions of people in a very short span of time. As with most incidents of this nature, the actual bug was small but caused countless issues across the country. According to an article from Stanford Report, an update to CrowdStrike’s Endpoint Detection and Response (EDR) software caused a crash, which caused a crash in the Windows system as well. The reason a small bug in this EDR software caused all of Windows OS to crash is because this software is used for cybersecurity purposes. Windows needs it to be constantly running at all times as part of their operating system in order for it to catch any security issues. As a result, Microsoft software could not run when EDR crashed (Durumeric, 2024). Microsoft is widely used across the world, so many systems were heavily impacted by the bug and were forced to spend time and resources on fixing it as soon as possible.

According to the statement provided from CrowdStrike on their own website, the bug was caused by an update to a sensor first created in February of 2024. The sensor was created to notice new techniques that could attack certain weaknesses in Windows software. The update differed from the previous code in the number of inputs expected. There were supposed to be 20, but the update gave 21 instead. In their words, “the mismatch resulted in an out-of-bounds memory read, causing a system crash” (*CrowdStrike,* 2024). In other words, the update tried to access a part of code that did not exist, which caused a crash. This crash had a widespread effect, particularly in sectors such as air travel. Delta was especially impacted, saying that over half of their systems use Windows (Durumeric, 2024). Many flights were cancelled since the fix was not immediately available and took time to administer. According to the Stanford Report, this took a long time because Windows requires a manual reboot into a mode that is safe to be able to delete the update, since rebooting the computer normally causes it to crash again. There are a few other sectors that were impacted, such as health care and banking, according to CNN. Health care is reported to lose around $1.94 billion, while banking lost around $1.15 billion (Fung, 2024). Clearly, this incident impacted more than just the company whose mistake it was.

The mistake was noticed only an hour and a half after the update was sent out, but systems had already updated automatically (Fung, 2024). There are many solutions for preventing this in the future. Obviously, CrowdStrike will be improving their testing and making sure another bug is not sent out at all. However, the companies using their software also could have used more preventative measures. It would be beneficial for Windows, at least, to improve their testing to make sure that updates are functional before they are installed. If systems being updated had flagged the update and paused before installing it, the problem could have been avoided. Preventative measures are very important in cases like this, since the faulty update was only released for an hour and a half before it had huge global impact. Systems like this cannot rely on feedback after they are released, which is why testing is so important. Testing has to be specific and purposeful, since anything that slips through the cracks can cause software companies and their clients to lose billions of dollars.

In conclusion, the CrowdStrike software incident had lasting impacts due to a small error. Even though it was pulled back quickly, it caused numerous issues in sectors such as air travel, health care, and banking. Ironically, the faulty update was intended to protect against unique attacks but ended up crashing all updated Windows systems. This crash will have impacts on future testing practices, since it became clear very quickly how many industries are completely reliant on software. As software continues to grow and develop, it is crucial that people understand how fragile our systems are and how heavily reliant we are on them. Becoming reliant on systems we do not understand is dangerous and will continue to cause bigger and bigger mishaps if people are not prepared for things to go wrong. Computer scientists and software engineers have a responsibility to build reliable software and reliable ways to test it so that further incidents of this nature can be avoided.

**References**

Durumeric, Z. (2024, July 26). *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

*Falcon Content Update Remediation and guidance hub: CrowdStrike*. crowdstrike.com. (2024, August 19). https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

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