acm U.S. Technology Policy Committee

August 11, 2024

STATEMENT ON MASS CYBERSECURITY INCIDENTS LIKELY TO RECUR
FULL AND TRANSPARENT INVESTIGATION REQUIRED

The ACM U.S. Technology Policy Committee (USTPC)[1] notes that the recent CrowdStrike incident reveals once again the complex interdependencies and apparent fragility of our global computing and communications infrastructure. That a piece of commercial software designed to help companies deal with malicious attacks would itself, by accident, cause outages that inflict losses of such scale is ironic, to say the least. But to computer scientists familiar with the underlying technology and the forces driving its development and deployment, it is not especially surprising, and future incidents are, unfortunately, almost a certainty.

Late on July 18, 2024 (CDT), CrowdStrike released a sensor configuration update to its Falcon detection and response service, which was distributed and automatically installed on client systems[2]. The update caused a global outage affecting an estimated 8.5 million computers including several critical infrastructure sectors: airlines, 911 emergency systems, banks, government agencies, healthcare and hospital systems around the world.[3,4] Although CrowdStrike noticed the error and pulled back the update within less than two hours, the damage took days to repair. The estimated cost of the damage worldwide is many billions of dollars, as has been widely reported.[5] CrowdStrike's management has issued an apology,

[1] The Association for Computing Machinery (ACM), with more than 100,000 members worldwide, is the world's largest educational and scientific computing society. ACM's US Technology Policy Committee (USTPC), currently comprising more than 160 members, serves as the focal point for ACM's interaction with all branches of the US government, the computing community, and the public on policy matters related to information technology. This Statement's principal authors for USTPC are Carl Landwehr and Jody Westby. Andrew Grosso, Jim Hendler, Jeanna Matthews, Stuart Shapiro, Gene Spafford, and Alec Yasinsac provided helpful comments.

[2] "Technical Details: Falcon Content Update for Windows Hosts," CrowdStrike Blog, July 20, 2024, https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/.

[3] Joe Tidy, "CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says," BBC News, July 20, 2024, https://www.bbc.com/news/articles/cpe3zgznwjno.

[4] Eva Rothenberg, "How the CrowdStrike outage unfolded – a timeline," CNN, July 20, 2024, https://www.eastidahonews.com/2024/07/how-the-crowdstrike-outage-unfolded-a-timeline/.

[5] Reuters, "Fortune 500 firms to see $5.4 bln in CrowdStrike losses, says insurer Parametrix," 24 July 2024. https://www.reuters.com/technology/fortune-500-firms-see-54-bln-crowdstrike-losses-says-insurer-parametrix-2024-07-24/

assured the public that this was not a cyberattack, and provided some detail as to how the accident happened.[6]

The flawed CrowdStrike update crashed thousands of Microsoft Windows-based systems, while systems based on Linux, Mac OS, and other operating systems were unaffected.[7] Understanding the underlying technical and perhaps policy reasons for the different system responses is crucial if we are to create a more resilient global cyberinfrastructure.[8]

The global nature of the outage highlights the need for improved international cooperation and coordination. The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) provided online links to information from other governmental cyber centers in the UK, Australia, and Canada.[9] While helpful, the ability of companies globally to obtain information about the outage, government efforts, and technical guidance was largely deficient, and each country and company was on its own – particularly if their systems were down. Legislators and regulators in countries with affected operations surely will be examining how best to protect their companies and citizens from similar outages going forward.

It is crucial that the details concerning how this error occurred be thoroughly and publicly investigated so that system operators, and technologists and policymakers as well, can draw from this incident the lessons needed to strengthen our cyberinfrastructure, improve incident response programs and remediation processes, develop protocols for automatic software updates, improve international coordination and cooperation, and develop claims processes for such incidents. Questions to be addressed include:

- How did some systems avoid the consequences of this error, while others did not?
- Why was the errant software released without thorough testing?
- What lessons can we draw concerning the architecture and implementation of systems?
- What best practices should be followed for automatic system updates?
- Why were some systems able to come back up faster than others?
- What were the most efficient ways to restart systems that required manual intervention?
- What notification should be required?

[6] "External Root Cause Analysis – Channel File 291," CrowdStrike. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

[7] Lily Hay Newman, Matt Burgess, Andy Greenburg, *Wired*. "How One Bad CrowdStrike Update Crashed the World's Computers," July 19. 2024. https://www.wired.com/story/crowdstrike-outage-update-windows/

[8] "Blue screens everywhere are latest woe for Microsoft," Tom Dotan and Robert McMillan, Wall Street Journal, July 21, 2024. https://www.wsj.com/tech/cybersecurity/microsoft-tech-outage-role-crowdstrike-50917b90

[9] "Widespread IT Outage Due to CrowdStrike Update," Cybersecurity and Infrastructure Security Agency, July 26, 2024, https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

- Where were gaps in international coordination an issue and how can they be closed?

Fortunately, the U.S. government has recently created an organization that appears uniquely positioned to undertake such an investigation and publish the results: the Cyber Safety Review Board (CSRB), operated by CISA.[10] The ACM USTPC urges that the necessary resources be made available to the CSRB so that this investigation can be undertaken promptly, thoroughly, and publicly. In addition, the ACM USTPC and Europe TPC membership stands ready to provide expertise where needed and assist in examining the foregoing issues and others. Our members bring deep technical, legal, operational, and managerial experience to multidisciplinary issues such as these.

[10] U.S. Department of Homeland Security. Cyber Safety Review Board Charter. Sept. 21, 2023, https://www.cisa.gov/sites/default/files/2023-09/CSRB%20Charter%2009.21.2023%20APPROVED_508c.pdf