NetChoice

September 23, 2024

Dear Chairman Green, Ranking Member Thompson, and Members of the Committee on Homeland Security:

I'm writing to you on behalf of NetChoice, a trade association that works to make the internet safe for free enterprise and free expression. We applaud the Committee's willingness to investigate the cause of the July 2024 Windows outage that affected 8.5 million Microsoft devices and cost at least $5 billion.[1] [2] The Committee's summoning of Crowdstrike to testify in the September 24 hearing is a good start.

However, Microsoft's role in government technology and its recent, repeated cybersecurity failures should also be reviewed in relation to this outage. Consider the following:

- Microsoft provides 85% of the U.S. government's productivity software, including Outlook, Word, Excel, and Teams.[3]
- According to the Cybersecurity & Infrastructure Security Agency, Microsoft software and services have accounted for 25% of all known exploited vulnerabilities since 2021.[4]
- Microsoft pledged to put security "above all else" in May.[5] Since that time, there have been 65 security incidents or vulnerabilities according to MicrosoftVulnerabilityTracker.com, a website NetChoice launched to highlight the risks of the government's overreliance on Microsoft.[6]

While the July outage wasn't Microsoft's fault, the government's overreliance on Microsoft's Windows Server allowed the outage to inflict widespread problems on America's critical IT infrastructure. The next outage could be caused by a nation-state attack, another faulty update from a third-party vendor, or other sources. Because so much of the U.S. government's software runs on Microsoft's systems, it is critical that Congress provide oversight to ensure the company is upholding the highest security standards.

---

[1] Microsoft says about 8.5 million of its devices affected by CrowdStrike-related outage (Jul. 20, 2024), https://www.reuters.com/technology/microsoft-says-about-85-million-its-devices-affected-by-crowdstrike-related-2024-07-20

[2] We finally know what caused the global tech outage - and how much it cost (Jul. 24, 2024), https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html

[3] Monoculture and market share: The state of communications and collaboration software in the US government (Sept. 21, 2021), https://omdia.tech.informa.com/-/media/tech/omdia/marketing/commissioned-research/pdfs/monoculture-and-market-share-the-state-of-communications-and-collaboration-software-in-the-us-government-v3.pdf?rev=8d41cc2d16de491b9f59d2906309fdaa

[4] Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[5] Prioritizing security above all else (May 3, 2024), https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else/

[6] Microsoft Vulnerability Tracker, https://microsoftvulnerabilitytracker.com/

Recently, NetChoice conducted research with Echelon Insights among 1,031 registered voters about the outage and found that the public shares our concerns about Microsoft's cybersecurity flaws and the government's overreliance on the company's software and services. Some key findings:

- 67% believe Microsoft is very or somewhat responsible for the outage.
- 62% were more concerned after the outage about Microsoft's market share in government and critical infrastructure software and services.
- 72% want the U.S. Congress to learn more about why the U.S. government is so reliant on Microsoft.

In June, the committee held a hearing with Brad Smith, Vice Chair and President of Microsoft, about "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security." Committee members raised important concerns about Microsoft's cybersecurity track record, monoculture over government technology, efforts to stifle competition, and significant connections to China, all of which threaten U.S. national security. But this latest attack shows that more oversight is needed.

Just a few months after launching its Secure Future Initiative,[7] Microsoft suffered yet another attack by Russian-sponsored group Nobelium, this time allowing foreign state-sponsored hackers to access critical email traffic between Microsoft and federal agencies.[8] And several times a week on average since the Initiative launch, Microsoft remains the victim of a number of exploited vulnerabilities and system breaches.[9]

It is critical to U.S. government cybersecurity that the Committee continue to conduct oversight of Microsoft and American IT procurement more broadly to ensure that our nation's tech infrastructure remains secure and protected at the highest standards. We thank you in advance for your continued attention to this matter.

Amy Bos
Director of State and Federal Affairs, NetChoice

NetChoice is a trade association that works to protect free expression and promote free enterprise online.

---

[7] Announcing Microsoft Secure Future Initiative to advance security engineering (Nov. 3, 2023), https://www.microsoft.com/en-us/security/blog/2023/11/02/announcing-microsoft-secure-future-initiative-to-advance-security-engineering/
[8] Federal government affected by Russian breach of Microsoft (Apr. 4, 2024), https://cyberscoop.com/federal-government-russian-breach-microsoft/
[9] Microsoft Vulnerability Tracker, https://microsoftvulnerabilitytracker.com/