THREAT REPORT: Severe Risk from Zero-Click Windows Vulnerability CVE-2024-38063

August 22, 2024

TLP: WHITE

Source: Zero-Click Exploit Concerns Drive Urgent Patching of Windows TCP/IP Flaw | SecurityWeek

Overview:

Security experts are urgently advising Windows system administrators to address a critical pre-auth remote code execution vulnerability in the Windows TCP/IP stack, identified as CVE-2024-38063. Microsoft has rated this flaw with a CVSS score of 9.8/10, highlighting its potential for zero-click exploitation—an exploit that requires no user interaction—through crafted IPv6 packets.

Chinese researcher Xiao Wei discovered this vulnerability "several months ago," a detail of critical significance given concerns about China stockpiling zero-day vulnerabilities for use by Advanced Persistent Threats (APTs). This practice is supported by the Cyberspace Administration of China's (CAC) mandate, effective September 2021, which requires that vulnerabilities be reported to the government within two days of discovery and prohibits sharing this information without explicit permission.

It is possible that this vulnerability has been added to the toolkit of China-affiliated APTs. While there is no confirmed exploitation in the wild yet, the CAC has had access to this vulnerability for several months, and it could have been used during this period.

What to Communicate to Executives:

- **Recommendation:** If IPv6 is necessary on your systems, ensure that you apply the latest patches to safeguard your systems. If IPv6 is not in use on your systems, it should be disabled to avoid risk. This practice aligns with good security measures, such as limiting system functions, and will protect against future attacks.
- **Impact:** Exploiting this vulnerability allows a remote attacker to execute code on any affected Windows system without needing user interaction. If exploited by China-based APTs, the likely impacts include serious espionage-related consequences, such as a complete loss of confidentiality.
- **Targeting:** If you are in an industry preferentially targeted by the Chinese government, then you are at heightened risk. Preferred targets include those that provide the Chinese government with strategic advantage such as energy and utilities, government, information and communication technology, military and defense, and advancement and research sectors.

Further Reading:

- New Law Will Help Chinese Government Stockpile Zero-Days | SecurityWeek
- China's Cyber Laws and Regulation | Margin Research
- CVE-2024-38063 – Security Update Guide | Microsoft

CYBER ALBERTA