Health-ISAC
Collaborating for Resilience in Healthcare

VULNERABILITY BULLETINS

Critical TCP/IP RCE on IPv6-Enabled Systems

○○○ TLP:WHITE

Aug 15, 2024

On August 13, 2024, Microsoft released a patch for a critical Windows TCP/IP Remote Code Execution Vulnerability labeled CVE-2024-38063. The vulnerability, which carries a CVSS score of 9.8, arises from an Integer Underflow weakness. This flaw allows unauthenticated attackers to trigger buffer overflows and execute arbitrary code on Windows 10, Windows 11, and Windows Server systems.

Unauthenticated attackers can remotely exploit the vulnerability through low-complexity attacks involving specially crafted IPv6 packets. The Microsoft advisory emphasizes the high risk of exploitation, supported by Trend Micro's Zero Day Initiative analysis, which has flagged CVE-2024-38063 as a particularly severe, wormable flaw.

Microsoft has addressed multiple IPv6-related vulnerabilities, including CVE-2020-16898/9 and CVE-2021-24086, underscoring the ongoing security challenges associated with the IPv6 protocol. One recommended temporary mitigation outside of patching is disabling IPv6 on an affected system. However, Microsoft states that IPv6 is integral to many Windows components, and disabling it could affect system functionality.

Recommendations

To mitigate the risk of exploitation, users should consider applying the latest Windows security updates listed in the Security Updates section of the Microsoft advisory.

Users who can not immediately install the updates can also disable IPv6 temporarily as a short-term mitigation. However, this is not recommended as a long-term solution because IPv6 is a mandatory part of various Windows products and versions, and disabling it could cause Windows components to stop working.

Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Microsoft Blog, Security Week, Security Online, Bleeping Computer, NCSC, HHS

Alert ID 1433ea0b

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags CVE-2024-38063, IPv6, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.