Multiple Vulnerabilities (RCE) In Microsoft Products

Vairav Advisory Report

Date: February 07, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

Multiple vulnerabilities have been identified in Microsoft Edge (Chromium-based), posing risks of remote code execution (RCE). These vulnerabilities, including CVE-2025-21283, CVE-2025-21408, CVE-2025-21342, and CVE-2025-21279, primarily stem from insufficient memory protections and type confusion flaws. Microsoft has released patches, and users are advised to apply updates immediately to mitigate potential security risks.

VULNERABILITY DETAILS

CVE-2025-21283

Description: A vulnerability caused by insufficient granularity of address regions protected by register locks.

Impact: Remote Code Execution (RCE).

CVSS Score: 6.5 (Medium)

CVE-2025-21408

Description: A vulnerability due to type confusion, allowing access to resources using incompatible types.

Impact: Remote Code Execution (RCE).

CVSS Score: 8.8 (High)

CVE-2025-21342

Description: Another vulnerability that allows unauthorized access and potential execution of malicious code.

Impact: Remote Code Execution (RCE)

CVSS Score: 8.8 (High)

CVE-2025-21279

Description: A vulnerability caused by type confusion, allowing improper access to resources using incompatible types.

Impact: Remote Code Execution (RCE).

CVSS Score: 6.5 (Medium)

AFFECTED VERSIONS

- Microsoft Edge (Chromium-based) from version 1.0.0 before 133.0.3065.51

EXPLOIT DETAILS

These vulnerabilities can be exploited through malicious web content, crafted network requests, or privilege escalation attacks. Successful exploitation may lead to remote code execution or unauthorized system access.

RECOMMENDED ACTIONS

- Microsoft has released patches to mitigate these vulnerabilities. Users should upgrade to the latest available versions of their affected products.

ADDITIONAL SECURITY MEASURES

- Limit administrative access and apply the principle of least privilege (PoLP).
- Configure browser security settings to block untrusted content.

REFERENCES

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21283

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21408

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21342

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21279

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com