CVE-2025-21355: Microsoft Bing Remote Code Execution Vulnerability

Vairav Advisory Report

Date: 2025-02-20

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

A critical vulnerability, identified as CVE-2025-21355, has been discovered in Microsoft Bing. This flaw allows unauthorized attackers to execute arbitrary code remotely over a network due to missing authentication for a critical function. The vulnerability has been assigned a CVSS v3.1 base score of 8.6 (High). Exploitation of this vulnerability could lead to significant security breaches, including unauthorized system access and data compromise.

VULNERABILITY DETAILS

CVE-2025-21355

- **Description:** The vulnerability stems from a missing authentication mechanism in a critical function within Microsoft Bing. This oversight permits attackers to send specially crafted requests over the network, leading to the execution of arbitrary code without requiring authentication.
- **Impact:** Successful exploitation allows attackers to execute malicious code remotely, potentially compromising system integrity, accessing sensitive data, and disrupting services.
- **CVSS Score:** 8.6 (High)

AFFECTED VERSIONS

All versions of Microsoft Bing prior to the security update released on February 19, 2025, are affected by this vulnerability.

EXPLOIT DETAILS

In real-world scenarios, attackers can exploit this vulnerability by sending crafted network requests to the vulnerable Bing service, bypassing authentication checks. This could lead to unauthorized code execution, allowing attackers to manipulate search results, exfiltrate data, or disrupt services. The vulnerability is particularly concerning for environments where Bing is integrated into enterprise applications, as exploitation could compromise connected systems and data.

RECOMMENDED ACTIONS

Microsoft did not require any intervention from end users or administrators since the fix was applied server-side.

ADDITIONAL SECURITY MEASURES

- **Review Logs**: Examine system and network logs for any unusual or suspicious activity related to Bing API requests around the time the vulnerability might have been exploited.
- **Monitor Data Flows**: Ensure that data from Bing-integrated applications is not showing unexpected patterns or outputs.
- **Update Cached Data**: Refresh any cached data or stored API responses from Bing to eliminate the possibility of lingering exploit remnants.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-21355
- https://windowsforum.com/threads/critical-microsoft-bing-vulnerability-cve-2025-21355-impact-and-mitigation-guide.352748/?utm_source=rss&utm_medium=rss
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21355

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: sales@vairavtech.com

Website: https://vairavtech.com