CVE-2025-24043: MICROSOFT WINDBG SOS DEBUGGING EXTENSION RCE

Vairav CVE Report

Date: March 12th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability, **CVE-2025-24043**, has been identified in Microsoft's WinDbg debugger, specifically within the SOS debugging extension. This flaw allows authenticated attackers with network access to execute arbitrary code remotely, posing significant risks such as system compromise and data breaches. The vulnerability has been assigned a CVSS score of 7.5, indicating high severity.

VULNERABILITY DETAILS

CVE-2025-24043

- **Description:** The vulnerability arises from improper verification of cryptographic signatures in the SOS debugging extension of WinDbg. This flaw enables attackers to bypass authentication mechanisms, allowing the execution of malicious code over a network.
- **Impact:** Exploitation of this vulnerability can lead to unauthorized remote code execution, potentially resulting in full system compromise, data theft, and disruption of services.
- **CVSS Score:** 7.5 (High)

AFFECTED VERSIONS

The following WinDbg packages are affected:

- **dotnet-sos:** Versions before 9.0.607501
- **dotnet-dump:** Versions before 9.0.557512
- **dotnet-debugger-extensions:** Version 9.0.557512

EXPLOIT DETAILS

Attackers with network access can exploit this vulnerability by initiating specially crafted debugging sessions that leverage the improper cryptographic signature verification in the SOS extension. Successful exploitation grants the attacker SYSTEM-level privileges on the affected Windows host.

RECOMMENDED ACTIONS

Users and organizations are strongly advised to upgrade to the latest versions of the affected packages:

- **dotnet-sos:** Upgrade to version 9.0.607501
- **dotnet-dump:** Upgrade to version 9.0.607501
- **dotnet-debugger-extensions:** Upgrade to version 9.0.607601

ADDITIONAL SECURITY MEASURES

- **Network Segmentation**: Implement network segmentation to limit access to critical systems and reduce the attack surface.
- **Access Controls**: Enforce strict access controls and least privilege principles to minimize the potential impact of exploitation.
- **Monitoring and Logging**: Enhance monitoring and logging to detect and respond to suspicious activities promptly.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-24043
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24043

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