CVE-2025-24043: MICROSOFT WINDBG SOS DEBUGGING EXTENSION REMOTE CODE EXECUTION VULNERABILITY

Vairav CVE Report

Date: March 11, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Microsoft has disclosed a critical security vulnerability (CVE-2025-24043) affecting its WinDbg debugger. This vulnerability stems from improper cryptographic signature verification within the SOS debugging extension, potentially enabling remote code execution (RCE) by an authenticated attacker. With a CVSS score of 7.5, exploitation of this flaw could allow unauthorized code execution over a network, posing significant risks to affected systems. Organizations using WinDbg for debugging applications, drivers, and Windows kernel-level issues must take immediate action to mitigate this threat.

VULNERABILITY DETAILS

CVE-2025-24043: Microsoft WinDbg SOS Debugging Extension Remote Code Execution Vulnerability

Description: The vulnerability arises from a flaw in how the SOS debugging extension within WinDbg verifies cryptographic signatures. Attackers with network access can bypass authentication, leading to unauthorized remote code execution. Microsoft has not identified any mitigating factors, increasing the urgency of remediation.

Impact: Unauthorized remote code execution, potential system compromise.

CVSS Score: 7.5 (High)

AFFECTED VERSIONS

This vulnerability affects Microsoft .NET Core projects referencing the following WinDbg packages:

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

EXPLOIT DETAILS

- Attackers with network access can exploit this vulnerability to execute arbitrary code.
- Exploitation could allow threat actors to bypass cryptographic verification mechanisms.

- No mitigations or workarounds have been identified by Microsoft, increasing the risk level.

RECOMMENDED ACTIONS

Microsoft strongly recommends upgrading to the latest secure versions:

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

ADDITIONAL SECURITY MEASURES

- Limit access to WinDbg debugging environments from untrusted sources.
- Enforce strict cryptographic signature verification policies.
- Implement logging and monitoring for unauthorized debugging attempt

REFERENCES

https://securityonline.info/windbg-remote-code-execution-vulnerability-cve-2025-24043-exposes-critical-security-risk/

https://github.com/dotnet/diagnostics/security/advisories/GHSA-hpw7-8qpc-34p3

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