Microsoft Windows Hyper-V NT Kernel Integration VSP Zero-Day Vulnerabilities

Overview

This week, Microsoft patched three zero-days within the Windows Hyper-V NT Kernel Integration VSP (CVE-2025-21333, CVE-2025-21334, CVE-2025-21335). These vulnerabilities are currently being exploited in the wild and could allow attackers to gain SYSTEM privileges.

Vulnerability Breakdown

- **CVEs** - CVE-2025-21333, CVE-2025-21334, CVE-2025-21335
- **Severity** - CVSS score 7.8
- **Vulnerability Type** - Elevation of Privilege
- **Affected Components** - Windows Hyper-V NT Kernel Integration VSP
- **Impact -** Successful exploitation grants SYSTEM privileges on affected machines.

Affected Products

- Windows Server 2025
- Windows 11 Version 24H2 (x64 and ARM64-based Systems)
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 10 Version 22H2 for x64-based Systems

If left unpatched, attackers might gain complete control over systems, leading to stolen data or malware spread across your network.

Aspire Protects

- **Patch –** Microsoft has issued patched for all three vulnerabilities. You may find patch guidance in Microsoft's advisories.
  - CVE-2025-21335
  - CVE-2025-21334
  - CVE-2025-21333
- As required by CISA, federal agencies must ensure these patches are implemented by February 4, 2025, to comply with the Known Exploited Vulnerabilities Catalog mandates.

- To see other Aspire Emergency Flash Notice's, please visit Aspire's Managed Services Customer Portal.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers could leverage existing footholds or use phishing tactics to execute code or commandeer accounts on affected systems.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – Attackers exploit these vulnerabilities to gain higher-level privileges which could be used to further the intrusion within the network.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Based on the usage of Microsoft products, potential industries could include

- Healthcare
- Finance
- Education
- Manufacturing
- Government
- Small to Medium Sized Businesses (SMBs)
- Transportation
- Retail
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2025-21335 - Security Update Guide - Microsoft - Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability

CVE-2025-21333 - Security Update Guide - Microsoft - Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability

CVE-2025-21334 - Security Update Guide - Microsoft - Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability

Zero Day Initiative — The January 2025 Security Update Review

Patch Tuesday January 2025 | Action1