Active Exploitation of Windows Kernel Elevation of Privilege Vulnerability

TL;DR

CVE-2025-62215 is a Windows kernel vulnerability attackers are already exploiting. Patch the affected Windows 11 and Windows Server systems now.

Overview

Microsoft's November 2025 Patch Tuesday release includes 63 vulnerabilities across Windows, Office, Visual Studio, Nuance PowerScribe, DirectX, and related components. Among these, a vulnerability tracked as CVE-2025-62215 (CVSS 7.8) is being exploited in the wild. The vulnerability is a Windows Kernel elevation of privilege flaw that impacts Windows 11 and Windows Server.

Affected Products

- Windows 11 Version 23H2 (x64 / ARM64)
- Windows 11 Version 24H2 (x64 / ARM64)
- Windows 11 Version 25H2 (x64 / ARM64)
- Windows Server 2022, 23H2 (Server Core)
- Windows Server 2025

CVE-2025-62215 is an elevation of privilege vulnerability in the Windows Kernel caused by a race condition and improper memory handling that can result in conditions such as double free. A local attacker with low privileges who already has code execution on a vulnerable system can trigger this flaw to corrupt kernel memory and gain SYSTEM-level access.

This vulnerability does not grant initial access, but it turns any low-privilege foothold into full SYSTEM control, which lets attackers disable defenses and pivot. If a threat actor exploits CVE-2025-62215, they can stop or tamper with security tools, dump credentials, and install persistent backdoors. Microsoft patched several other bugs this month, like GDI+, Office, and Visual Studio issues, but CVE-2025-62215 is the one that

needs priority. Because the vulnerability impacts Windows and Windows Server, Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Patch CVE-2025-62215 immediately. See Microsoft's security advisory for more information.
- Tighten local accounts and admin use, restrict arbitrary software execution where possible.
- Review exposed services that routinely handle untrusted code or users.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit CVE-2025-62215 on a compromised Windows host to gain SYSTEM-level privileges.

Defense Evasion

- Impair Defenses [T1562] – With SYSTEM access, the attacker may stop or alter security tools, logging, or monitoring to remain undetected.

Credential Access

- OS Credential Dumping [T1003] – After elevation, the attacker may dump credentials (e.g., LSASS memory) to expand access across the environment.

IoCs

There are no known IoCs associated with the above vulnerability 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

This vulnerability is relevant to any organization running modern Windows:

- Finance
- Government
- Education

- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's 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-2025-62215 - Security Update Guide - Microsoft - Windows Kernel Elevation of Privilege Vulnerability

November 2025 Microsoft Patch Tuesday | Tenable®