.

VULNERABILITY BULLETINS

An Elevation of Privilege Zero-Day Vulnerability in Microsoft's Windows Kernel (CVE-2025-62215)

TLP:WHITE

Nov 12, 2025

On November 11, 2025, Microsoft publicly disclosed a high-severity Elevation of Privilege (EoP) zero-day vulnerability found in the Windows Kernel, tracked as **CVE-2025-62215** (CVSS Score: 7.0). Microsoft also released a patch for the vulnerability on the same date.

Microsoft has not disclosed any information regarding the attacks that exploit the vulnerability, although it has confirmed that this flaw is actively being exploited in the wild.

Health-ISAC is sharing this information to increase situational awareness and encourage organizations to assess their risk level associated with this vulnerability.

Analysis

CVE-2025-62215 is an Elevation of Privilege (EoP) zero-day vulnerability found in the Windows Kernel. On November 11, 2025, it was publicly disclosed and patched as part of the November 2025 Patch Tuesday update, with Microsoft confirming it had been actively exploited in the wild.

The flaw is categorized as a high-severity race condition caused by improper synchronization when handling shared resources in the Kernel. Successful exploitation allows an authenticated, local attacker to gain SYSTEM privileges on the compromised Windows device, requiring them to win the race condition. However, the attacker must already have Local Access and Low Privileges on the targeted Windows system. This means the zero-day is typically used as the second stage in an attack chain, following an initial compromise, such as successful phishing or malware delivery.

The vulnerability affects a wide range of currently supported Microsoft Windows operating systems, including both client and server editions, as it resides in the core Windows Kernel. The impacted versions that received a patch on November 11, 2025, include:

- Windows 11 (versions 22H2, 23H2, and 24H2)
- Windows 10 (all supported versions, including those enrolled in the Extended Security Updates (ESU) program, such as version 22H2)
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

Because this is a fundamental flaw in the Windows Kernel, any supported operating system using the vulnerable component requires the immediate security update to mitigate the active exploitation risk.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Prioritize patching and conduct a risk assessment for your systems.
- Enforce strict Least Privilege (Zero Trust) by implementing Role-Based Access Controls (RBAC) and Application Control.
- Strictly enforce network segmentation.
- Leverage advanced Endpoint Detection and Response (EDR).
- Maintain a continuous, real-time asset inventory of all software and devices.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	securityweek, hhs, microsoft
Tactics-Techniques-Sub-techniques	• Enterprise - TA0002: Execution - T1203: Exploitation for Client Execution • Enterprise - TA0004: Privilege Escalation - T1068: Exploitation for Privilege Escalation • Enterprise - TA0005: Defense Evasion - T1548: Abuse Elevation Control Mechanism - T1548.002: Bypass User Account Control

Alert ID 36420abd

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-62215, Elevation of Privilege, Windows Kernel, Zero-Day, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.