EnCyb

Severity: High

Advisory Type: Security

Windows Kernel Elevation of Privilege Vulnerability

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

CVE-2025-62215 is an actively exploited Windows Kernel zero-day (race condition + double-free) that allows a local, low-privilege user to escalate to system.

- CVE ID: CVE-2025-62215
- Active Region: Global
- Affected Sector: All Sectors
- Affected Product: Windows 10 (ESU), Windows 11, Windows Server 2019, 2022, 2025
- Severity: High (CVSS: 7.0)
- Published Date: November 11, 2025

TECHNICAL DETAILS

- Microsoft patched a Windows kernel elevation-of-privilege (EoP) bug that stems from improper synchronization / race conditions in a kernel component, allowing memory-corruption (use-after-free / out-of-bounds) style impacts when abused.
- The bug was confirmed as a 0-day actively exploited in the wild prior to the November patch, prompting Microsoft to include it in the Patch Tuesday fixes.
- Exploits observed enable a local attacker (or an already-compromised low-privilege process) to escalate to SYSTEM/kernel privileges, enabling persistence, full system control, and potential payloads (code execution, further lateral movement). It's typically chained after achieving code execution in user context.
- Microsoft released patches (KB5068858, KB5068859, KB5068860, KB5068861, KB5068862, KB5068865) and short-term mitigations include restricting access to untrusted local accounts/processes, applying EDR/kernel-hardening protections, and enforcing least privilege/patch management for endpoint fleets.

IMPACT

- Full system compromise via kernel mode code execution
- Escalation to SYSTEM privileges
- Theft of credentials and authentication artifacts
- Lateral movement across the network
- Persistent backdoors or kernel implants
- Large scale ransomware deployment or data exfiltration

RECOMMENDATIONS

- Apply November 2025 Windows updates to all affected hosts. Refer the Microsoft link: *https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215*
- Prioritize patching domain controllers, admin/jump hosts, and internet-facing servers.
- Restrict local user privileges and enforce least privilege access.
- Rotate credentials and investigate any signs of prior exploitation.
- Implement application allowlisting and block execution of untrusted binaries.

REFERENCES

- https://nvd.nist.gov/vuln/detail/CVE-2025-62215
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com