Windows Kernel Elevation of Privilege Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40369
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:16 UTC
Updated	2026-05-12 18:17:16 UTC
Description	Untrusted pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from secure@microsoft.com

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-822 | CWE-822 CWE-822: Untrusted Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Windows 11 Version 24H2	affected 10.0.26100.0 10.0.26100.8457 custom	ARM64-based Syst
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.8457 custom	ARM64-based Syst
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.2113 custom	ARM64-based Syst
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32860 custom	x64-based Systems
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32860 custom	x64-based Systems

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40369	secure@microsoft.com	msrc.microsoft.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.