Windows Volume Manager Extension Driver Remote Code Execution Vulnerability

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

Summary

CVE	CVE-2026-40380
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:16 UTC
Updated	2026-05-13 15:34:52 UTC
Description	Heap-based buffer overflow in Volume Manager Extension Driver allows an authorized attacker to execute code with a phys

Risk And Classification

Primary CVSS: v3.1 6.2 MEDIUM from secure@microsoft.com

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

Problem Types: CWE-122 | CWE-125 | CWE-197 | CWE-122 CWE-122: Heap-based Buffer Overflow | CWE-125 CWE-125: Out-of-bounds Read | CWE-197 CWE-197: Numeric Truncation Error

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	6.2	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.2	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfo
CNA	Microsoft	Windows 10 Version 1607	affected 10.0.14393.0 10.0.14393.9140 custom	32-bit
CNA	Microsoft	Windows 10 Version 1809	affected 10.0.17763.0 10.0.17763.8755 custom	32-bit
CNA	Microsoft	Windows 10 Version 21H2	affected 10.0.19044.0 10.0.19044.7291 custom	32-bit
CNA	Microsoft	Windows 10 Version 22H2	affected 10.0.19045.0 10.0.19045.7291 custom	32-bit
CNA	Microsoft	Windows 11 Version 22H3	affected 10.0.22631.0 10.0.22631.7079 custom	ARM6
CNA	Microsoft	Windows 11 Version 23H2	affected 10.0.22631.0 10.0.22631.7079 custom	x64-b
CNA	Microsoft	Windows 11 Version 24H2	affected 10.0.26100.0 10.0.26100.8457 custom	ARM6
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.8457 custom	ARM6
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.2113 custom	ARM6
CNA	Microsoft	Windows Server 2012	affected 6.2.9200.0 6.2.9200.26079 custom	x64-b
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected 6.2.9200.0 6.2.9200.26079 custom	x64-b
CNA	Microsoft	Windows Server 2012 R2	affected 6.3.9600.0 6.3.9600.23181 custom	x64-b
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected 6.3.9600.0 6.3.9600.23181 custom	x64-b
CNA	Microsoft	Windows Server 2016	affected 10.0.14393.0 10.0.14393.9140 custom	x64-b
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected 10.0.14393.0 10.0.14393.9140 custom	x64-b
CNA	Microsoft	Windows Server 2019	affected 10.0.17763.0 10.0.17763.8755 custom	x64-b
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected 10.0.17763.0 10.0.17763.8755 custom	x64-b
CNA	Microsoft	Windows Server 2022	affected 10.0.20348.0 10.0.20348.5139 custom	x64-b
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.2330 custom	x64-b
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32860 custom	x64-b
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32860 custom	x64-b

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40380	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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**