



Windows Common Log File System Driver Elevation of Privilege Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-40407
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:18 UTC
Updated	2026-05-15 15:19:29 UTC
Description	Heap-based buffer overflow in Windows Common Log File System Driver allows an authorized attacker to elevate privilege:

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

EPSS: 0.000440000 probability, percentile 0.135380000 (date 2026-05-14)

Problem Types: CWE-122 | CWE-122 CWE-122: Heap-based Buffer Overflow

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10 1607	All	All	All	All
Operating System	Microsoft	Windows 10 1607	All	All	All	All
Operating System	Microsoft	Windows 10 1809	All	All	All	All
Operating System	Microsoft	Windows 10 1809	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 11 23h2	All	All	All	All
Operating System	Microsoft	Windows 11 23h2	All	All	All	All
Operating System	Microsoft	Windows 11 24h2	All	All	All	All
Operating System	Microsoft	Windows 11 24h2	All	All	All	All
Operating System	Microsoft	Windows 11 25h2	All	All	All	All
Operating System	Microsoft	Windows 11 25h2	All	All	All	All
Operating System	Microsoft	Windows 11 26h1	All	All	All	All
Operating System	Microsoft	Windows 11 26h1	All	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2019	All	All	All	All
Operating System	Microsoft	Windows Server 2022	All	All	All	All
Operating System	Microsoft	Windows Server 2022 23h2	All	All	All	All
Operating System	Microsoft	Windows Server 2025	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
--------	--------	---------	---------	----------

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	ARM64
CNA	Microsoft	Windows 11 Version 23H2	affected	10.0.22631.0	10.0.22631.7079	custom	x64-bit
CNA	Microsoft	Windows 11 Version 24H2	affected	10.0.26100.0	10.0.26100.8457	custom	ARM64
CNA	Microsoft	Windows 11 Version 25H2	affected	10.0.26200.0	10.0.26200.8457	custom	ARM64
CNA	Microsoft	Windows 11 Version 26H1	affected	10.0.28000.0	10.0.28000.2113	custom	ARM64
CNA	Microsoft	Windows Server 2012	affected	6.2.9200.0	6.2.9200.26079	custom	x64-bit
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected	6.2.9200.0	6.2.9200.26079	custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2	affected	6.3.9600.0	6.3.9600.23181	custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected	6.3.9600.0	6.3.9600.23181	custom	x64-bit
CNA	Microsoft	Windows Server 2016	affected	10.0.14393.0	10.0.14393.9140	custom	x64-bit
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected	10.0.14393.0	10.0.14393.9140	custom	x64-bit
CNA	Microsoft	Windows Server 2019	affected	10.0.17763.0	10.0.17763.8755	custom	x64-bit
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected	10.0.17763.0	10.0.17763.8755	custom	x64-bit
CNA	Microsoft	Windows Server 2022	affected	10.0.20348.0	10.0.20348.5139	custom	x64-bit
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected	10.0.25398.0	10.0.25398.2330	custom	x64-bit
CNA	Microsoft	Windows Server 2025	affected	10.0.26100.0	10.0.26100.32860	custom	x64-bit
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected	10.0.26100.0	10.0.26100.32860	custom	x64-bit

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40407	secure@microsoft.com	msrc.microsoft.com	Vendor Advisory
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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