



Windows Common Log File System Driver Elevation of Privilege Vulnerability

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

Summary

CVE	CVE-2023-36424
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-14 18:15:45 UTC
Updated	2026-04-14 14:44:43 UTC
Description	Windows Common Log File System Driver Elevation of Privilege Vulnerability

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.055450000 probability, percentile 0.902830000 (date 2026-04-20)

CISA KEV: Listed on 2026-04-13; due 2026-04-27; ransomware use Unknown

Problem Types: CWE-125 | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	secure@microsoft.com	Secondary	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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Out-of-Bounds Read Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36424 ; https://nvd.nist.gov/vuln/detail/CVE-2023-36424

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10 1507	All	All	All	All
Operating System	Microsoft	Windows 10 1507	All	All	All	All
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 1809	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 11 21h2	All	All	All	All
Operating System	Microsoft	Windows 11 22h2	All	All	All	All
Operating System	Microsoft	Windows 11 23h2	All	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Microsoft	Windows 11 Version 22H3	affected 10.0.22631.0 10.0.22631.2715 custom
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.531 custom
CNA	Microsoft	Windows 11 Version 23H2	affected 10.0.22631.0 10.0.22631.2715 custom
CNA	Microsoft	Windows 10 Version 1809	affected 10.0.17763.0 10.0.17763.5122 custom
CNA	Microsoft	Windows 10 Version 1809	affected 10.0.0 10.0.17763.5122 custom
CNA	Microsoft	Windows Server 2019	affected 10.0.17763.0 10.0.17763.5122 custom
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected 10.0.17763.0 10.0.17763.5122 custom
CNA	Microsoft	Windows Server 2022	affected 10.0.20348.0 10.0.20348.2113 custom
CNA	Microsoft	Windows 11 Version 21H2	affected 10.0.0 10.0.22000.2600 custom
CNA	Microsoft	Windows 10 Version 21H2	affected 10.0.19043.0 10.0.19043.3693 custom
CNA	Microsoft	Windows 11 Version 22H2	affected 10.0.22621.0 10.0.22621.2715 custom
CNA	Microsoft	Windows 10 Version 22H2	affected 10.0.19045.0 10.0.19045.3693 custom
CNA	Microsoft	Windows 10 Version 1507	affected 10.0.10240.0 10.0.10240.20308 custom
CNA	Microsoft	Windows 10 Version 1607	affected 10.0.14393.0 10.0.14393.6452 custom
CNA	Microsoft	Windows Server 2016	affected 10.0.14393.0 10.0.14393.6452 custom
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected 10.0.14393.0 10.0.14393.6452 custom
CNA	Microsoft	Windows Server 2008 Service Pack 2	affected 6.0.6003.0 6.0.6003.22367 custom
CNA	Microsoft	Windows Server 2008 Service Pack 2 Server Core Installation	affected 6.0.6003.0 6.0.6003.22367 custom
CNA	Microsoft	Windows Server 2008 Service Pack 2	affected 6.0.6003.0 6.0.6003.22367 custom
CNA	Microsoft	Windows Server 2008 R2 Service Pack 1	affected 6.1.7601.0 6.1.7601.26816 custom
CNA	Microsoft	Windows Server 2008 R2 Service Pack 1 Server Core Installation	affected 6.1.7601.0 6.1.7601.26816 custom
CNA	Microsoft	Windows Server 2012	affected 6.2.9200.0 6.2.9200.24569 custom
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected 6.2.9200.0 6.2.9200.24569 custom
CNA	Microsoft	Windows Server 2012 R2	affected 6.3.9600.0 6.3.9600.21668 custom
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected 6.3.9600.0 6.3.9600.21668 custom

References

Reference	Source	Link	Tags
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Govern
Security Update Guide - Microsoft Security Response Center	af854a3a-2127-422b-91ae-364da2661108	msrc.microsoft.com	Patch, Ver

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-04-13T00:00:00.000Z	CVE-2023-36424 added to CISA KEV

Legacy QID Mappings

92075 Microsoft Windows Security Update for November 2023

92081 Microsoft Azure Stack Hub Security Updates for November 2023

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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