



# Windows Kerberos Elevation of Privilege Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-27912
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 18:16:58 UTC
<b>Updated</b>	2026-04-17 15:10:35 UTC
<b>Description</b>	Improper authorization in Windows Kerberos allows an authorized attacker to elevate privileges over an adjacent network.

## Risk And Classification

**Primary CVSS:** v3.1 8 HIGH from secure@microsoft.com

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

**EPSS:** 0.002670000 probability, percentile 0.501770000 (date 2026-04-21)

**Problem Types:** CWE-285 | CWE-285 CWE-285: Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	8	HIGH	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8	HIGH	CVSS:3.1/AV:A/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

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

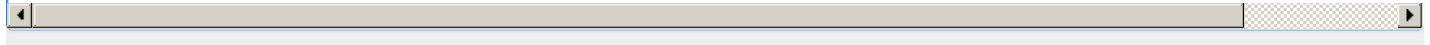
High

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Microsoft	Windows Server 2012	affected 6.2.9200.0 6.2.9200.26026 custom	x64-b
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected 6.2.9200.0 6.2.9200.26026 custom	x64-b
CNA	Microsoft	Windows Server 2012 R2	affected 6.3.9600.0 6.3.9600.23132 custom	x64-b
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected 6.3.9600.0 6.3.9600.23132 custom	x64-b
CNA	Microsoft	Windows Server 2016	affected 10.0.14393.0 10.0.14393.9060 custom	x64-b
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected 10.0.14393.0 10.0.14393.9060 custom	x64-b
CNA	Microsoft	Windows Server 2019	affected 10.0.17763.0 10.0.17763.8644 custom	x64-b
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected 10.0.17763.0 10.0.17763.8644 custom	x64-b
CNA	Microsoft	Windows Server 2022	affected 10.0.20348.0 10.0.20348.5020 custom	x64-b
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.2274 custom	x64-b
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b



References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-27912	secure@microsoft.com	<a href="https://msrc.microsoft.com">msrc.microsoft.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© 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 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](https://cve.report/api)

