Windows Netlogon Remote Code Execution Vulnerability

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

Summary

CVE	CVE-2026-41089
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:20 UTC
Updated	2026-05-15 15:42:17 UTC
Description	Stack-based buffer overflow in Windows Netlogon allows an unauthorized attacker to execute code over a network.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from secure@microsoft.com

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

EPSS: 0.000930000 probability, percentile 0.259510000 (date 2026-05-14)

Problem Types: CWE-121 | CWE-121 CWE-121: Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 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	Platfc
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-2026-41089	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.

Free CVE JSON API cve.report/api

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