



Windows Snipping Tool Spoofing Vulnerability

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

Summary

CVE	CVE-2026-33829
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 18:17:35 UTC
Updated	2026-04-21 14:16:04 UTC
Description	Exposure of sensitive information to an unauthorized actor in Windows Snipping Tool allows an unauthorized attacker to pe

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from secure@microsoft.com

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

EPSS: 0.000690000 probability, percentile 0.212160000 (date 2026-04-20)

Problem Types: CWE-200 | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

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	10.0.14393.9060	custom	32-bit
CNA	Microsoft	Windows 10 Version 1809	affected	10.0.17763.0	10.0.17763.8644	custom	32-bit
CNA	Microsoft	Windows 10 Version 21H2	affected	10.0.19044.0	10.0.19044.7184	custom	32-bit
CNA	Microsoft	Windows 10 Version 22H2	affected	10.0.19045.0	10.0.19045.7184	custom	32-bit
CNA	Microsoft	Windows 11 Version 22H3	affected	10.0.22631.0	10.0.22631.6936	custom	ARM64
CNA	Microsoft	Windows 11 Version 23H2	affected	10.0.22631.0	10.0.22631.6936	custom	x64-bit
CNA	Microsoft	Windows 11 Version 24H2	affected	10.0.26100.0	10.0.26100.8246	custom	ARM64
CNA	Microsoft	Windows 11 Version 25H2	affected	10.0.26200.0	10.0.26200.8246	custom	ARM64
CNA	Microsoft	Windows 11 Version 26H1	affected	10.0.28000.0	10.0.28000.1836	custom	ARM64
CNA	Microsoft	Windows Server 2012	affected	6.2.9200.0	6.2.9200.26026	custom	x64-bit
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected	6.2.9200.0	6.2.9200.26026	custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2	affected	6.3.9600.0	6.3.9600.23132	custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected	6.3.9600.0	6.3.9600.23132	custom	x64-bit
CNA	Microsoft	Windows Server 2016	affected	10.0.14393.0	10.0.14393.9060	custom	x64-bit
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected	10.0.14393.0	10.0.14393.9060	custom	x64-bit
CNA	Microsoft	Windows Server 2019	affected	10.0.17763.0	10.0.17763.8644	custom	x64-bit
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected	10.0.17763.0	10.0.17763.8644	custom	x64-bit
CNA	Microsoft	Windows Server 2022	affected	10.0.20348.0	10.0.20348.5020	custom	x64-bit
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected	10.0.25398.0	10.0.25398.2274	custom	x64-bit
CNA	Microsoft	Windows Server 2025	affected	10.0.26100.0	10.0.26100.32690	custom	x64-bit
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected	10.0.26100.0	10.0.26100.32690	custom	x64-bit

References

Reference	Source	Link
github.com/blackarrowsec/redteam-research/tree/master/CVE-2026-33829	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33829	secure@microsoft.com	msrc.microsoft.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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

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