



Windows Remote Desktop Services Elevation of Privilege Vulnerability

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

Summary

CVE	CVE-2026-21533
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-10 18:16:35 UTC
Updated	2026-03-30 13:27:43 UTC
Description	Improper privilege management in Windows Remote Desktop allows an authorized attacker to elevate privileges locally.

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: 0.196140000 probability, percentile 0.953810000 (date 2026-04-01)

CISA KEV: Listed on 2026-02-10; due 2026-03-03; ransomware use Unknown

Problem Types: CWE-269 | CWE-269 CWE-269: Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
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:F/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 Improper Privilege Management 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/vulnerability/CVE-2026-21533 ; https://nvd.nist.gov/vuln/detail/CVE-2026-21533

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 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 10.0.14393.8868 custom	32-bit
CNA	Microsoft	Windows 10 Version 1809	affected 10.0.17763.0 10.0.17763.8389 custom	32-bit
CNA	Microsoft	Windows 10 Version 21H2	affected 10.0.19044.0 10.0.19044.6937 custom	32-bit
CNA	Microsoft	Windows 10 Version 22H2	affected 10.0.19045.0 10.0.19045.6937 custom	32-bit
CNA	Microsoft	Windows 11 Version 22H3	affected 10.0.22631.0 10.0.22631.6649 custom	ARM64
CNA	Microsoft	Windows 11 Version 23H2	affected 10.0.22631.0 10.0.22631.6649 custom	x64-bit
CNA	Microsoft	Windows 11 Version 24H2	affected 10.0.26100.0 10.0.26100.7840 custom	ARM64
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.7840 custom	Not specified
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.1575 custom	ARM64
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.1575 custom	Not specified
CNA	Microsoft	Windows Server 2012	affected 6.2.9200.0 6.2.9200.25923 custom	x64-bit
CNA	Microsoft	Windows Server 2012 Server Core Installation	affected 6.2.9200.0 6.2.9200.25923 custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2	affected 6.3.9600.0 6.3.9600.23022 custom	x64-bit
CNA	Microsoft	Windows Server 2012 R2 Server Core Installation	affected 6.3.9600.0 6.3.9600.23022 custom	x64-bit
CNA	Microsoft	Windows Server 2016	affected 10.0.14393.0 10.0.14393.8868 custom	x64-bit
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected 10.0.14393.0 10.0.14393.8868 custom	x64-bit
CNA	Microsoft	Windows Server 2019	affected 10.0.17763.0 10.0.17763.8389 custom	x64-bit
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected 10.0.17763.0 10.0.17763.8389 custom	x64-bit
CNA	Microsoft	Windows Server 2022	affected 10.0.20348.0 10.0.20348.4773 custom	x64-bit
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.2149 custom	x64-bit
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32370 custom	x64-bit
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32370 custom	x64-bit

References

Reference	Source	Link
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533	secure@microsoft.com	msrc.microsoft.com
www.vicarius.io/vsociety/posts/cve-2026-21533-mitigation-script-privilege-esc...	af854a3a-2127-422b-91ae-364da2661108	www.vicarius.io
www.vicarius.io/vsociety/posts/cve-2026-21533-detection-script-privilege-esca...	af854a3a-2127-422b-91ae-364da2661108	www.vicarius.io

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

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-02-10T00:00:00.000Z	CVE-2026-21533 added to CISA KEV

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

© [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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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