



FreeRDP: DoS via WINPR_ASSERT in rts_read_auth_verifier_no_checks

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

Summary

CVE	CVE-2026-33952
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 22:16:18 UTC
Updated	2026-04-01 20:06:42 UTC
Description	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, an unvalidated auth_length field

Risk And Classification

Primary CVSS: v4.0 6 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000630000 probability, percentile 0.195210000 (date 2026-04-01)

Problem Types: CWE-617 | CWE-617 CWE-617: Reachable Assertion

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/
4.0	CNA	DECLARED	6	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freerdp	Freerdp	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CVE-2024-3010	Freerdp	Freerdp	0.15.0-0.16.0	Windows, Linux

CNA

FreeRDP

FreeRDP

affected < 3.24.2

Not specified

References

Reference	Source	Link
github.com/FreeRDP/FreeRDP/commit/4ac0b6467d371a1ad47c1f751c5b305e4c068adb	security-advisories@github.com	github.com
github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4v4p-9v5x-hc93	security-advisories@github.com	github.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.

© 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)