



FreeRDP: Persistent Cache bmpSize Desync - Heap OOB Write

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

Summary

CVE	CVE-2026-33987
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 22:16:20 UTC
Updated	2026-04-01 18:44:43 UTC
Description	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, in persistent_cache_read_entry

Risk And Classification

Primary CVSS: v3.1 6.6 MEDIUM from nvd@nist.gov

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

EPSS: 0.000130000 probability, percentile 0.020600000 (date 2026-04-01)

Problem Types: CWE-122 | CWE-131 | CWE-122 CWE-122: Heap-based Buffer Overflow | CWE-131 CWE-131: Incorrect Calculation of Buffer Size

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H
3.1	security-advisories@github.com	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/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
CNA	FreeRDP	FreeRDP	affected < 3.24.2	Not specified

References

Reference	Source	Link	T
github.com/FreeRDP/FreeRDP/security/advisories/GHSA-ff8h-p5vc-wcwc	security-advisories@github.com	github.com	P
github.com/FreeRDP/FreeRDP/commit/1a890eb43492b5eb707cb3dd6fc908f696e8fc1c	security-advisories@github.com	github.com	P
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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](#)