



CVE-2022-41877

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

Summary

CVE	CVE-2022-41877
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-16 20:15:00 UTC
Updated	2024-01-12 13:15:00 UTC
Description	FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input length validation.

Risk And Classification

Problem Types: CWE-1284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Freerdp	Freerdp	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 37 Update: freerdp-2.9.0-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 36 Update: freerdp-2.9.0-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
FreeRDP: Multiple Vulnerabilities (GLSA 202401-16) — Gentoo security		security.gentoo.org
[SECURITY] Fedora 36 Update: freerdp-2.9.0-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[debian-lts-announce] 20231117 [SECURITY] [DLA 3654-1] freerdp2 security update		lists.debian.org
[SECURITY] Fedora 37 Update: freerdp-2.9.0-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Missing input length validation in `drive` channel · Advisory · FreeRDP/FreeRDP · GitHub	CONFIRM	github.com
Fixed missing stream length check in drive_file_query_directory · FreeRDP/FreeRDP@6655841 · GitHub	MISC	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.

Legacy QID Mappings

160601 Oracle Enterprise Linux Security Update for freerdp (ELSA-2023-2326)
160676 Oracle Enterprise Linux Security Update for freerdp (ELSA-2023-2851)
182690 Debian Security Update for freerdp2 (CVE-2022-41877)
199966 Ubuntu Security Notification for FreeRDP Vulnerabilities (USN-6522-1)
199988 Ubuntu Security Notification for FreeRDP Vulnerabilities (USN-6522-2)
241431 Red Hat Update for freerdp (RHSA-2023:2326)
241541 Red Hat Update for freerdp (RHSA-2023:2851)
283518 Fedora Security Update for freerdp (FEDORA-2022-fd6e43dec8)
283519 Fedora Security Update for freerdp (FEDORA-2022-076b1c9978)
354723 Amazon Linux Security Advisory for freerdp : ALAS2-2023-1930
378638 Alibaba Cloud Linux Security Update for freerdp (ALINUX3-SA-2023:0064)
502855 Alpine Linux Security Update for freerdp
6000329 Debian Security Update for freerdp2 (DLA 3654-1)
672604 EulerOS Security Update for freerdp (EulerOS-SA-2023-1313)
691013 Free Berkeley Software Distribution (FreeBSD) Security Update for freerdp (1f0421b1-8398-11ed-973d-002b67dfc673)
710834 Gentoo Linux FreeRDP Multiple Vulnerabilities (GLSA 202401-16)
753679 SUSE Enterprise Linux Security Update for freerdp (SUSE-SU-2023:0400-1)
753682 SUSE Enterprise Linux Security Update for freerdp (SUSE-SU-2023:0399-1)
941031 AlmaLinux Security Update for freerdp (ALSA-2023:2326)
941069 AlmaLinux Security Update for freerdp (ALSA-2023:2851)

© [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](#)