



CVE-2020-15103

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-15103
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-27 18:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All Fre

Risk And Classification

Problem Types: CWE-680

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Freerdp	Freerdp	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link
USN-4481-1: FreeRDP vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com

FreeRDP security and version 2.2.0 release by bmiklautz · Pull Request #6382 · FreeRDP/FreeRDP · GitHub	MISC	github.com
FreeRDP/ChangeLog at 616af2d5b86dc24c7b3e89870dbcffd841d9a535 · FreeRDP/FreeRDP · GitHub	MISC	github.com
[SECURITY] Fedora 32 Update: freerdp-2.2.0-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: freerdp-2.2.0-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: freerdp-2.2.0-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:1332-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] [DLA 3606-1] freerdp2 security update	MLIST	lists.debian.org
[SECURITY] Fedora 31 Update: freerdp-2.2.0-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Integer overflow in RDPE GFX channel · Advisory · FreeRDP/FreeRDP · GitHub	CONFIRM	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

[159221](#) Oracle Enterprise Linux Security Update for freerdp (ELSA-2021-1849)

[239295](#) Red Hat Update for freerdp (RHSA-2021:1849)

[500966](#) Alpine Linux Security Update for freerdp

[6000137](#) Debian Security Update for freerdp2 (DLA 3606-1)

[671555](#) EulerOS Security Update for freerdp (EulerOS-SA-2022-1564)

[690484](#) Free Berkeley Software Distribution (FreeBSD) Security Update for freerdp (a955cdb7-d089-11ea-8c6f-080027eedc6a)

[750634](#) OpenSUSE Security Update for freerdp (openSUSE-SU-2020:1332-1)

[940286](#) AlmaLinux Security Update for freerdp (ALSA-2021:1849)

[960882](#) Rocky Linux Security Update for freerdp (RLSA-2021:1849)

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

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