



CVE-2024-22211

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-22211
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-19 20:15:00 UTC
Updated	2024-01-26 20:24:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	L
Integer Overflow leading to Heap Overflow in freerdp_bitmap_planar_context_reset · Advisory · FreeRDP/FreeRDP · GitHub		gi
[codec,planar] check resolution for overflow · FreeRDP/FreeRDP@aeac304 · GitHub		gi
[codec,planar] check resolution for overflow · FreeRDP/FreeRDP@939e922 · GitHub		gi
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [284920](#) Fedora Security Update for freerdp (FEDORA-2024-f294ddb7fb)
- [285003](#) Fedora Security Update for freerdp (FEDORA-2024-01689e51e5)
- [510802](#) Alpine Linux Security Update for freerdp
- [755857](#) SUSE Enterprise Linux Security Update for freerdp (SUSE-SU-2024:0649-1)

755858 SUSE Enterprise Linux Security Update for freerdp (SUSE-SU-2024:0648-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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