



CVE-2020-29260

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

Summary

CVE	CVE-2020-29260
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-02 23:15:00 UTC
Updated	2022-10-05 20:56:00 UTC
Description	libvncclient v0.9.13 was discovered to contain a memory leak via the function rfbClientCleanup().

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Libvncserver Project	Libvncserver	0.9.13	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3125-1] libvncserver security update	MLIST	lists.debian.org	
libvncclient: free vncRec memory in rfbClientCleanup() · LibVNC/libvncserver@bef41f6 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [181098](#) Debian Security Update for libvncserver (DLA 3125-1)
- [355698](#) Amazon Linux Security Advisory for libvncserver : ALAS2-2023-2170
- [502882](#) Alpine Linux Security Update for libvncserver
- [752854](#) SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2022:3990-1)

752976 SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2022:4330-1)

752976 SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2022:4330-1)

753328 SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2022:3540-1)

© [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](#).

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