



# CVE-2020-25708

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

## Summary

<b>CVE</b>	CVE-2020-25708
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-27 18:15:00 UTC
<b>Updated</b>	2022-10-29 02:41:00 UTC
<b>Description</b>	A divide by zero issue was found to occur in libvncserver-0.9.12. A malicious client could use this flaw to send a specially c

## Risk And Classification

**Problem Types:** CWE-369

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Libvncserver Project</a>	<a href="#">Libvncserver</a>	0.9.12	All	All	All
Application	<a href="#">Libvncserver Project</a>	<a href="#">Libvncserver</a>	0.9.12	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

Reference	Source
[SECURITY] [DLA 3125-1] libvncserver security update	MLIST
1896739 – (CVE-2020-25708) CVE-2020-25708 libvncserver: libvncserver/rfbserver.c has a divide by zero which could result in DoS	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159219](#) Oracle Enterprise Linux Security Update for libvncserver (ELSA-2021-1811)

[181098](#) Debian Security Update for libvncserver (DLA 3125-1)

[239298](#) Red Hat Update for libvncserver (RHSA-2021:1811)

[377567](#) Alibaba Cloud Linux Security Update for gnome (ALINUX3-SA-2022:0108)

[501068](#) Alpine Linux Security Update for libvncserver

[670189](#) EulerOS Security Update for libvncserver (EulerOS-SA-2021-1688)

[750536](#) OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:2097-1)

[750569](#) OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:2025-1)

[940381](#) AlmaLinux Security Update for libvncserver (ALSA-2021:1811)

[960345](#) Rocky Linux Security Update for libvncserver (RLSA-2021:1811)

© [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](#)