



# CVE-2020-14399

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

## Summary

<b>CVE</b>	CVE-2020-14399
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-17 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	** DISPUTED ** An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint32_t p

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Libvncserver Project</a>	<a href="#">Libvncserver</a>	All	All	All	All
Application	<a href="#">Libvncserver Project</a>	<a href="#">Libvncserver</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

### Reference

[security-announce] openSUSE-SU-2020:1056-1: important: Security update

[security-announce] openSUSE-SU-2020:0988-1: important: Security update

1860354 – (CVE-2020-14399) CVE-2020-14399 libvncserver: byte-aligned data is accessed through uint32\_t pointers in libvncclient/rfbproto.c

libvncclient: fix pointer aliasing/alignment issue · LibVNC/libvncserver@23e5cbe · GitHub

Comparing LibVNCServer-0.9.12...LibVNCServer-0.9.13 · LibVNC/libvncserver · GitHub

USN-4434-1: LibVNCServer vulnerabilities | Ubuntu security notices | Ubuntu

[SECURITY] [DLA 2264-1] libvncserver security update

[security-announce] openSUSE-SU-2020:1025-1: important: Security update

[SECURITY] [DLA 2347-1] libvncserver security update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

501068 Alpine Linux Security Update for libvncserver

© 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](#)**