



# CVE-2017-18922

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

## Summary

<b>CVE</b>	CVE-2017-18922
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-30 11:15:00 UTC
<b>Updated</b>	2023-11-07 02:41:00 UTC
<b>Description</b>	It was discovered that websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A

## Risk And Classification

**Problem Types:** CWE-787

## 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>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
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>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	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
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc1500</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc1500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc1500 Pro</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc1500 Pro Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc1900</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc1900 Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc1900 Pro</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc1900 Pro Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc2200</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc2200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Itc2200 Pro</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Itc2200 Pro Firmware</a>	All	All	All	All

## References

Reference	Source	Link
fix overflow and refactor websockets decode (Hybi) · LibVNC/libvncserver@aac95a9 · GitHub	MISC	<a href="#">github.com</a>
[security-announce] openSUSE-SU-2020:1056-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2020:0988-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2020:0978-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
USN-4407-1: LibVNCServer vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>
[SECURITY] Fedora 31 Update: libvncserver-0.9.13-2.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 32 Update: libvncserver-0.9.13-2.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: libvncserver-0.9.13-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
oss-security - libvncserver: old websocket decoding patch	MISC	<a href="#">www.openwall.com</a>
[security-announce] openSUSE-SU-2020:0960-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
1852356 – (CVE-2017-18922) CVE-2017-18922 libvncserver: websocket decoding buffer overflow	MISC	<a href="#">bugzilla.redhat.com</a>
[SECURITY] Fedora 32 Update: libvncserver-0.9.13-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2020:1025-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
oss-security - Re: libvncserver: old websocket decoding patch	MLIST	<a href="#">www.openwall.com</a>
<a href="#">cert-portal.siemens.com/productcert/pdf/ssa-390195.pdf</a>	CONFIRM	<a href="#">cert-portal.siemens.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377184](#) Alibaba Cloud Linux Security Update for libvncserver (ALINUX2-SA-2020:0111)

[590668](#) Siemens SIMATIC ITC Multiple Vulnerabilities (ICSA-21-350-12)

[940414](#) AlmaLinux Security Update for libvncserver (ALSA-2020:3385)

© [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](#)