



# CVE-2018-20023

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

## Summary

<b>CVE</b>	CVE-2018-20023
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnerability@kaspersky.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-19 16:29:00 UTC
<b>Updated</b>	2020-10-23 13:15:00 UTC
<b>Description</b>	LibVNC before 8b06f835e259652b0ff026898014fc7297ade858 contains CWE-665: Improper Initialization vulnerability in VI

## Risk And Classification

**Problem Types:** CWE-665

## 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>	14.04	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>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	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>	18.10	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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Libvnc Project</a>	<a href="#">Libvncserver</a>	All	All	All	All
Application	<a href="#">Libvnc Project</a>	<a href="#">Libvncserver</a>	All	All	All	All

## References

Reference	Source	Link	Tags
-----------	--------	------	------

USN-3877-1: LibVNCServer vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
KLCERT-18-033: LibVNC Memory leak   Kaspersky Lab ICS CERT	MISC	<a href="https://ics-cert.kaspersky.com">ics-cert.kaspersky.com</a>	Third Party Advisory
USN-4547-1: iTALC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
[SECURITY] [DLA 1979-1] italc security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
USN-4587-1: iTALC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
Debian -- Security Information -- DSA-4383-1 libvncserver	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
[SECURITY] [DLA 1617-1] libvncserver security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party
LibVNCServer: Multiple vulnerabilities (GLSA 201908-05) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[710154](#) Gentoo Linux LibVNCServer Multiple vulnerabilities (GLSA 201908-05)

© [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](#)