



# CVE-2019-15681

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

## Summary

<b>CVE</b>	CVE-2019-15681
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnerability@kaspersky.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-29 19:15:00 UTC
<b>Updated</b>	2022-04-05 21:10:00 UTC
<b>Description</b>	LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server

## 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>	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>	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="#">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>	0.9.12	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>	0.9.12	-	All	All

Application	<a href="#">Libvnc Project</a>	<a href="#">Libvncserver</a>	0.9.12	-	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>	15.1	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	Tags
[security-announce] openSUSE-SU-2020:1071-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing
[SECURITY] [DLA 2045-1] tightvnc security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing
[SECURITY] [DLA 1977-1] libvncserver security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing
USN-4547-1: iTALC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Pa
USN-4573-1: VINO vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Pa
rfbserver: don't leak stack memory to the remote · LibVNC/libvncserver@d01e1bb · GitHub	MISC	<a href="https://github.com">github.com</a>	Patch, T
USN-4407-1: LibVNCServer vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Pa
[SECURITY] [DLA 1979-1] italc security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing
USN-4587-1: iTALC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-390195.pdf">cert-portal.siemens.com/productcert/pdf/ssa-390195.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
[security-announce] openSUSE-SU-2020:0624-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing
[SECURITY] [DLA 2014-1] vino security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

501067 Alpine Linux Security Update for libvncserver

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

© [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](#)