



CVE-2018-7225

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

Summary

CVE	CVE-2018-7225
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-19 15:29:00 UTC
Updated	2020-10-23 13:15:00 UTC
Description	An issue was discovered in LibVNCServer through 0.9.11. rfbProcessClientNormalMessage() in rfbserver.c does not sanitiz

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libvncserver Project	Libvncserver	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference

[SECURITY] [DLA 2045-1] tightvnc security update

Malformed Request

USN-4547-1: iTALC vulnerabilities | Ubuntu security notices | Ubuntu

USN-4573-1: Vino vulnerabilities | Ubuntu security notices | Ubuntu

[SECURITY] [DLA 1332-1] libvncserver security update

[SECURITY] [DLA 1979-1] italc security update

oss-security - LibVNCServer rfbserver.c: rfbProcessClientNormalMessage() case rfbClientCutText doesn't sanitize msg.cct.length

USN-4587-1: iTALC vulnerabilities | Ubuntu security notices | Ubuntu

USN-3618-1: LibVNCServer vulnerability | Ubuntu security notices

Security: libvncserver/rfbserver.c: rfbProcessClientNormalMessage() case rfbClientCutText doesn't sanitize msg.cct.length · Issue #218 · LibV

Red Hat Customer Portal

LibVNCServer: Multiple vulnerabilities (GLSA 201908-05) — Gentoo security

[SECURITY] [DLA 2014-1] vino security update

Debian -- Security Information -- DSA-4221-1 libvncserver

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501066](#) Alpine Linux Security Update for libvncserver

[505049](#) 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](#)