CVE-2017-18922

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-18922
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-30 11:15:00 UTC
Updated	2023-11-07 02:41:00 UTC
Description	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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Libvncserver Project	Libvncserver	All	All	All	All
Application	Libvncserver Project	Libvncserver	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

Operating System	Opensuse	Leap	15.2	All	All	All
Hardware	Siemens	Simatic Itc1500	-	All	All	All
Operating System	Siemens	Simatic Itc1500 Firmware	All	All	All	All
Hardware	Siemens	Simatic Itc1500 Pro	-	All	All	All
Operating System	Siemens	Simatic Itc1500 Pro Firmware	All	All	All	All
Hardware	Siemens	Simatic Itc1900	-	All	All	All
Operating System	Siemens	Simatic Itc1900 Firmware	All	All	All	All
Hardware	Siemens	Simatic Itc1900 Pro	-	All	All	All
Operating System	Siemens	Simatic Itc1900 Pro Firmware	All	All	All	All
Hardware	Siemens	Simatic Itc2200	-	All	All	All
Operating System	Siemens	Simatic Itc2200 Firmware	All	All	All	All
Hardware	Siemens	Simatic Itc2200 Pro	-	All	All	All
Operating System	Siemens	Simatic Itc2200 Pro Firmware	All	All	All	All

References

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

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)