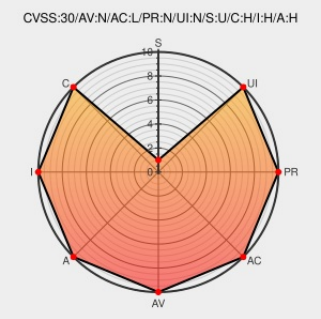
CVE-2018-15126

Published on: 12/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:26 PM UTC

CVE-2018-15126

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

LibVNC before commit 73cb96fec028a576a5a24417b57723b55854ad7b contains heap use-after-free vulnerability in server code of file transfer extension that can result remote code execution

CVE-2018-15126 has been assigned by vulnerability@kaspersky.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
USN-3877-1: LibVNCServer vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3877-1

[SECURITY] [DLA 1979-1] italc security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20191030 [SECURITY] [DLA 1979-1] italc security update
[SECURITY] [DLA 1652-1] libvncserver security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190131 [SECURITY] [DLA 1652-1] libvncserver security update
Debian -- Security Information -- DSA-4383-1 libvncserver	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4383
KLCERT-18-027: LibVNC Heap Use-After-Free | Kaspersky Lab ICS CERT	Third Party Advisory ics-cert.kaspersky.com text/html	MISC ics-cert.kaspersky.com/advisories/klcert-advisories/2018/12/19/klcert-18-027-libvnc-heap-use-after-free/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libvnc Project	Libvncserver	All	All	All	All

Application	Libvnc Project	Libvncserver	All	All	All	All
Application	Libvnc Project	Libvncserver	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:libvnc_project:libvncserver:*:*:*:*:*:*:*:*:

cpe:2.3:a:libvnc_project:libvncserver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→