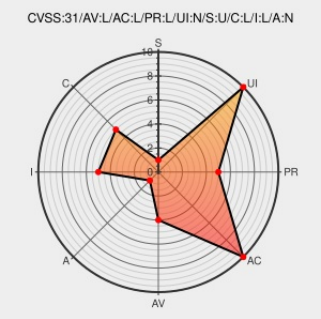
CVE-2020-13696

Published on: 06/08/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 07:30:00 PM UTC

CVE-2020-13696

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



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

An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command.

CVE-2020-13696 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.4 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link

xawtv3.git - xawtv 3.x	Patch Vendor Advisory git.linuxtv.org text/html	MISC git.linuxtv.org/xawtv3.git/commit/?id=36dc44e68e5886339b4a0fbe3f404fb1a4fd2292
[SECURITY] Fedora 31 Update: xawtv-3.107-2.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-93db553bb7
oss-security - xawtv: CVE-2020-13696: v4l-conf setuid-root program allows file existence tests and open(..., O_RDRW) on arbitrary files	Issue Tracking Mailing List Third Party Advisory www.openwall.com text/html	CONFIRM www.openwall.com/lists/oss-security/2020/06/04/6
[SECURITY] [DLA 2246-1] xawtv security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20200612 [SECURITY] [DLA 2246-1] xawtv security update
[security-announce] openSUSE-SU-2020:0787-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0787
[SECURITY] Fedora 32 Update: xawtv-3.107-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-cd5ad916e4
[security-announce] openSUSE-SU-2020:0784-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0784
xawtv3.git - xawtv 3.x	Patch Vendor Advisory git.linuxtv.org text/html	MISC git.linuxtv.org/xawtv3.git/commit/?id=31f31f9cbaee7be806cba38e0ff5431bd44b20a3
USN-4518-1: xawtv vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4518-1
Invalid Bug ID	Broken Link Third Party Advisory bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=CVE-2020-13696
xawtv3.git - xawtv 3.x	Patch Vendor Advisory git.linuxtv.org text/html	MISC git.linuxtv.org/xawtv3.git/commit/?id=8e3feea862db68d3ca0886f46cd99fab45d2db7c

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	16.04	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Linuxtv	Xawtv	All	All	All	All
Application	Linuxtv	Xawtv	All	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

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

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

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

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:a:linuxtv:xawtv:*:*:*:*:*:*:*:*:

cpe:2.3:a:linuxtv:xawtv:*:*:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report