

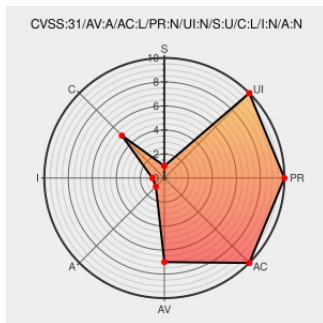


CVE-2020-12862

Published on: 06/24/2020 12:00:00 AM UTC

Last Modified on: 11/08/2022 03:32:00 AM UTC

CVE-2020-12862

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-082.

CVE-2020-12862 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GHSL-2020-075, GHSL-2020-079, GHSL-2020-080, GHSL-2020-081, GHSL-2020-082, GHSL-2020-083, GHSL-2020-084: Multiple vulnerabilities in SANE Backends (DoS, RCE) - GitHub Security Lab	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC securitylab.github.com/advisories/GHSL-2020-075-libsane

[security-announce] openSUSE-SU-2020:1791-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1791
[sane-announce] SANE Backends 1.0.30 security bug fix release	Mailing List Release Notes Third Party Advisory alioth-lists.debian.net text/html	 CONFIRM alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html
[SECURITY] [DLA 2332-1] sane-backends security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200817 [SECURITY] [DLA 2332-1] sane-backends security update
USN-4470-1: sane-backends vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4470-1
[SECURITY] [DLA 2332-2] sane-backends regression update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20201007 [SECURITY] [DLA 2332-2] sane-backends regression update
[security-announce] openSUSE-SU-2020:1798-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1798

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[501245](#) Alpine Linux Security Update for sane

[671604](#) EulerOS Security Update for sane-backends (EulerOS-SA-2022-1587)

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	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Sane-project	Sane Backends	All	All	All	All
Operating System	Sane-project	Sane Backends	All	All	All	All

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

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:*:*:*:
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:
cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:
cpe:2.3:o:sane-project:sane_backends:*:*:*:*:*:*:
cpe:2.3:o:sane-project:sane_backends:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		