CVE-2017-6318

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-6318
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-20 16:59:00 UTC
Updated	2020-09-01 14:15:00 UTC
Description	saned in sane-backends 1.0.25 allows remote attackers to obtain sensitive memory information via a crafted SANE_NET_C

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Application	Sane-backends Project	Sane-backends	1.0.25	All	All	All
Application	Sane-backends Project	Sane-backends	1.0.25	All	All	All

References

Reference
[sane-devel] Bug#854804: saned: SANE_NET_CONTROL_OPTION response packet may contain memory contents of the server
USN-4470-1: sane-backends vulnerabilities | Ubuntu security notices | Ubuntu
alioth.debian.org/tracker/index.php
[sane-devel] CVE-2017-6318 (old: Bug#854804: saned: SANE_NET_CONTROL_OPTION response packet may contain memory contents of
[sane-devel] Bug#854804: saned: SANE_NET_CONTROL_OPTION response packet may contain memory contents of the server
openSUSE-SU-2017:0649-1: moderate: Security update for sane-backends
sane-backends CVE-2017-6318 Information Disclosure Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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