CVE-2019-18932

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

Summary

CVE	CVE-2019-18932
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-21 18:15:00 UTC
Updated	2022-04-26 20:05:00 UTC
Description	log.c in Squid Analysis Report Generator (sarg) through 2.3.11 allows local privilege escalation. By default, it uses a fixed te

Risk And Classification

Problem Types: CWE-362 | CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Application	Squid Analysis Report Generator Project	Squid Analysis Report Generator	All	All	All	All

References

Reference
SourceForge.net: Project Info - sarg
oss-security - CVE-2019-18932: sarg: insecure usage of /tmp/sarg allows privilege escalation / DoS attack vector
Sarg: Local privilege escalation (GLSA 202007-32) — Gentoo security
[security-announce] openSUSE-SU-2020:0117-1: important: Security update
oss-security - Re: CVE-2019-18932: sarg: insecure usage of /tmp/sarg allows privilege escalation / DoS attack vector
[security-announce] openSUSE-SU-2020:0140-1: important: Security update
oss-sec: CVE-2019-18932: sarg: insecure usage of /tmp/sarg allows privilege escalation / DoS attack vector
Bug 1150554 – AUDIT-1: sarg: review of cron job file(s): /etc/cron.daily/suse.de-sarg, /etc/cron.monthly/suse.de-sarg, /etc/cron.weekly/suse.d
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**