CVE-2020-5202

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-5202
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-21 18:15:00 UTC
Updated	2022-01-01 20:03:00 UTC
Description	apt-cacher-ng through 3.3 allows local users to obtain sensitive information by hijacking the hardcoded TCP port. The /usr/l

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apt-cacher-ng Project	Apt-cacher-ng	All	All	All	All
Operating System	Debian	Debian Linux	10.0	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	10.0	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	Opensuse	Backports	sle-15	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference
[security-announce] openSUSE-SU-2020:0124-1: important: Security update
CVE-2020-5202
oss-security - CVE-2020-5202: apt-cacher-ng: a local unprivileged user can impersonate the apt-cacher-ng daemon, possible credentials leak
[security-announce] openSUSE-SU-2020:0146-1: important: Security update
oss-sec: CVE-2020-5202: apt-cacher-ng: a local unprivileged user can impersonate the apt-cacher-ng daemon, possible credentials leak

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.