



CVE-2022-23608

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23608
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-22 20:15:00 UTC
Updated	2023-08-30 01:15:00 UTC
Description	PJSIP is a free and open source multimedia communication library written in C language implementing standard based pro

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Certified Asterisk	All	All	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert1	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert10	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert11	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert12	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert2	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert3	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert4	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert5	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert6	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert7	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert8	All	All
Application	Asterisk	Certified Asterisk	16.8.0	cert9	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Sangoma	Asterisk	All	All	All	All
Application	Teluu	Pjsip	All	All	All	All

References

Reference	Source	Link	Tags
Asterisk Project Security Advisory - AST-2022-005 ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] [DLA 2962-1] pjproject security update	MLIST	lists.debian.org	
Full Disclosure: AST-2022-005: pjproject: undefined behavior after freeing a dialog set	FULLDISC	seclists.org	
PJSIP: Multiple Vulnerabilities (GLSA 202210-37) — Gentoo security	GENTOO	security.gentoo.org	
Use after free of dialog set · Advisory · pjsip/pjproject · GitHub	CONFIRM	github.com	
[SECURITY] [DLA 3549-1] ring security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5285-1 asterisk	DEBIAN	www.debian.org	
[SECURITY] [DLA 3194-1] asterisk security update	MLIST	lists.debian.org	
Merge pull request from GHSA-ffff-m5fm-qm62 · pjsip/pjproject@db32359 · GitHub	MISC	github.com	
[SECURITY] [DLA 2962-2] pjproject regression update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [179161](#) Debian Security Update for pjproject (DLA 2962-1)
- [179166](#) Debian Security Update for pjproject (DLA 2962-2)
- [181225](#) Debian Security Update for asterisk (DLA 3194-1)
- [181237](#) Debian Security Update for asterisk (DSA 5285-1)
- [182250](#) Debian Security Update for ring (CVE-2022-23608)
- [199817](#) Ubuntu Security Notification for Ring Vulnerabilities (USN-6422-1)
- [502231](#) Alpine Linux Security Update for pjproject
- [504292](#) Alpine Linux Security Update for pjproject
- [6000045](#) Debian Security Update for ring (DLA 3549-1)
- [690808](#) Free Berkeley Software Distribution (FreeBSD) Security Update for asterisk (964c5460-9c66-11ec-ad3a-001999f8d30b)
- [710674](#) Gentoo Linux PJSIP Multiple Vulnerabilities (GLSA 202210-37)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)