



CVE-2021-43804

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

Summary

CVE	CVE-2021-43804
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-22 18:15:00 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-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Teluu	Pjsip	All	All	All	All

References

Reference	Source	Link	Tags
Potential out-of-bounds read when parsing RTCP BYE message · Advisory · pjsip/pjproject · GitHub	CONFIRM	github.com	
[SECURITY] [DLA 2962-1] pjproject security update	MLIST	lists.debian.org	
PJSIP: Multiple Vulnerabilities (GLSA 202210-37) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] [DLA 3549-1] ring security update	MLIST	lists.debian.org	
Merge pull request from GHSA-3qx3-cg72-wrh9 · pjsip/pjproject@8b621f1 · GitHub	MISC	github.com	
Debian -- Security Information -- DSA-5285-1 asterisk	DEBIAN	www.debian.org	
[SECURITY] [DLA 3194-1] asterisk security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	cancel
NVD vulnerability detail	NVD	nvd.nist.gov	cancel

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179161	Debian Security Update for pjproject (DLA 2962-1)
181225	Debian Security Update for asterisk (DLA 3194-1)
181237	Debian Security Update for asterisk (DSA 5285-1)
183473	Debian Security Update for ring (CVE-2021-43804)
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)
710674	Gentoo Linux PJSIP Multiple Vulnerabilities (GLSA 202210-37)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)