



CVE-2023-27585

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

Summary

CVE	CVE-2023-27585
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-14 17:15:00 UTC
Updated	2023-08-30 01:15:00 UTC
Description	PJSIP is a free and open source multimedia communication library written in C. A buffer overflow vulnerability in versions 2.

Risk And Classification

Problem Types: CWE-120 | CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Teluu	Pjsip	All	All	All	All

References

Reference	Source	Link	Tags
DNS Asynchronous/Caching Resolution Engine (2.10)	MISC	www.pjsip.org	
Heap buffer overflow when parsing DNS packet (2) · Advisory · pjsip/pjproject · GitHub	MISC	github.com	
Debian -- Security Information -- DSA-5438-1 asterisk	DEBIAN	www.debian.org	
[SECURITY] [DLA 3394-1] asterisk security update	MLIST	lists.debian.org	
[SECURITY] [DLA 3549-1] ring security update	MLIST	lists.debian.org	
Merge pull request from GHSA-q9cp-8wcq-7pfr · pjsip/pjproject@d1c5e4d · GitHub	MISC	github.com	
Potential heap buffer overflow when parsing DNS packets · Advisory · pjsip/pjproject · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181742 Debian Security Update for asterisk (DLA 3394-1)
199817 Ubuntu Security Notification for Ring Vulnerabilities (USN-6422-1)
199901 Ubuntu Security Notification for Ring Vulnerabilities (USN-6422-2)
503543 Alpine Linux Security Update for pjproject
505918 Alpine Linux Security Update for pjproject
6000045 Debian Security Update for ring (DLA 3549-1)
6000231 Debian Security Update for asterisk (DSA 5438-1)

© [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](#)