# CVE-2021-43302

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-43302 |
| **State** | PUBLIC |
| **Assigner** | security@jfrog.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2022-02-16 21:15:00 UTC |
| **Updated** | 2023-08-30 01:15:00 UTC |
| **Description** | Read out-of-bounds in PJSUA API when calling pjsua_recorder_create. An attacker-controlled 'filename' argument may cau |

## 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 | 11.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Teluu | Pjsip | All | All | All | All |

## References

| Reference |
|---|
| [SECURITY] [DLA 2962-1] pjproject security update |
| Potential buffer overflow in pjsua_player_create(), pjsua_recorder_create(), pjmedia_wav_player_create(), and pjsua_call_dump() · Advisory · |
| [SECURITY] [DLA 3549-1] ring security update |
| Debian -- Security Information -- DSA-5285-1 asterisk |
| [SECURITY] [DLA 3194-1] asterisk security update |
| CVE Program record |
| NVD vulnerability detail |

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) |
| 182982 | Debian Security Update for ring (CVE-2021-43302) |
| 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) |

© 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 registred 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**