



CVE-2021-41141

Published on: 01/04/2022 12:00:00 AM UTC

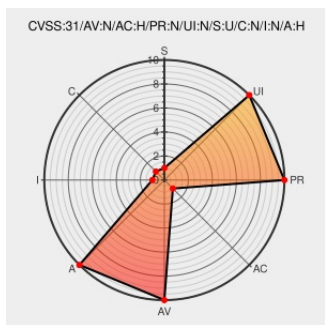
Last Modified on: 01/13/2022 06:33:00 PM UTC

CVE-2021-41141 - advisory for GHSA-8fmx-hqw7-6gmc

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Pjsip](#) from [Teluu](#) contain the following vulnerability:

PJSIP is a free and open source multimedia communication library written in the C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In various parts of PJSIP, when error/failure occurs, it is found that the function returns without releasing the currently held locks. This could result in a system deadlock, which cause a denial of service for the users. No release has yet been made which contains the linked fix commit. All versions up to an including 2.11.1 are affected. Users may need to manually apply the patch.

CVE-2021-41141 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [pjsip](#) - [pjproject](#) version <= 2.11.1

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Merge pull request from GHSA-8fmx-hqw7-6gmc · pjsip/pjproject@1aa2c0e · GitHub	github.com text/html	MISC github.com/pjsip/pjproject/commit/1aa2c0e0fb60a1b0bf793e0d834073ffe50fb196
Missing unreleased of locks in failure cases · Advisory · pjsip/pjproject · GitHub	github.com text/html	CONFIRM github.com/pjsip/pjproject/security/advisories/GHSA-8fmx-hqw7-6gmc

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Teluu	Pjsip	All	All	All	All
<pre>cpe:2.3:a:teluu:pjsip:*****:*</pre>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41141 : PJSIP is a free and open source multimedia communication library written in the C language impleme... twitter.com/i/web/status/1...	2022-01-04 18:45:36

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 |

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