



# CVE-2021-32686

Published on: 07/23/2021 12:00:00 AM UTC

Last Modified on: 08/05/2021 03:20:00 PM UTC

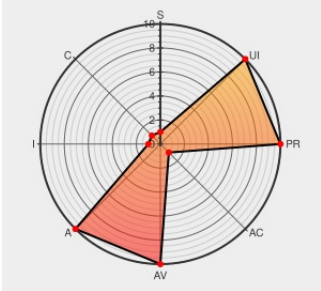
## CVE-2021-32686 - advisory for GHSA-cv8x-p47p-99wr

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In PJSIP before version 2.11.1, there are a couple of issues found in the SSL socket. First, a race condition between callback and destroy, due to the accepted socket having no group lock. Second, the SSL socket parent/listener

may get destroyed during handshake. Both issues were reported to happen intermittently in heavy load TLS connections. They cause a crash, resulting in a denial of service. These are fixed in version 2.11.1.

CVE-2021-32686 has been assigned by [security-advisories@github.com](mailto:security-advisories@github.com) to track the vulnerability - currently rated as **MEDIUM** severity.

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

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>NONE</b>	<b>HIGH</b>

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>NONE</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
Race condition in SSL socket server by nanangizz · Pull Request #2716 · pjsip/pjproject · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/pjsip/pjproject/pull/2716">github.com/pjsip/pjproject/pull/2716</a>
Merge pull request from GHSA-cv8x-p47p-99wr · pjsip/pjproject@d5f95aa · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/pjsip/pjproject/commit/d5f95aa066f878b0aef6a64e60b61e8626e664cd">github.com/pjsip/pjproject/commit/d5f95aa066f878b0aef6a64e60b61e8626e664cd</a>
Release PJSIP version 2.11.1 · pjsip/pjproject · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/pjsip/pjproject/releases/tag/2.11.1">github.com/pjsip/pjproject/releases/tag/2.11.1</a>
Race condition in SSL socket server · Advisory · pjsip/pjproject · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/pjsip/pjproject/security/advisories/GHSA-cv8x-p47p-99wr">github.com/pjsip/pjproject/security/advisories/GHSA-cv8x-p47p-99wr</a>

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](mailto:comment@cve.report).

## Related QID Numbers

- [690079](#) Free Berkeley Software Distribution (FreeBSD) Security Update for pjsip (92ad12b8-ec09-11eb-ae11-0897988a1c07)
- [690081](#) Free Berkeley Software Distribution (FreeBSD) Security Update for asterisk (53fbffe6-ebf7-11eb-ae11-0897988a1c07)

## Known Affected Configurations (CPE V2.3)

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

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32686 : PJSIP is a free and open source multimedia communication library written in C language implementin... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-07-23 21:38:37
/r/netcve	<a href="#">CVE-2021-32686</a>	2021-07-23 22:38:28

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

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](#)**