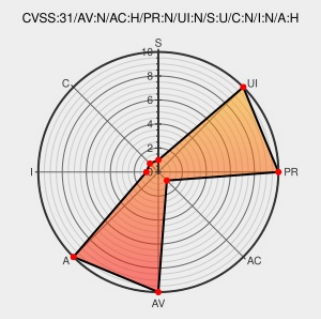
CVE-2021-32686

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



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 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
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

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

Related QID Numbers

690079 Free Berkeley Software Distribution (FreeBSD) Security Update for pjsip (92ad12b8-ec09-11eb-aef1-0897988a1c07)

690081 Free Berkeley Software Distribution (FreeBSD) Security Update for asterisk (53fbffe6-ebf7-11eb-aef1-0897988a1c07)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:teluu:pjsip:*:*:*:*:*:*:*:*:

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… twitter.com/i/web/status/1…	2021-07-23 21:38:37
/r/netcve	CVE-2021-32686	2021-07-23 22:38:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report