Asterisk ASTERISK-29057

pjsip: Crash on call rejection during high load

Details

Type:	Security	Status:	CLOSED
Severity:	Blocker	Resolution:	Fixed
Affects Version/s:	13.35.0, (2)	Target Release Version/s:	13.37.1, (8)
Component/s:	pjproject/pjsip		
Labels:	patch security		
Regression:	No		

Description

This is a crash within PJSIP whereby under heavy load the INVITE transaction on an INVITE session may not be set when sending a response, resulting in a crash.

Attachments

AST-2020-001.pdf	45 kB	29/Oct/20 11:49 AM
ASTERISK-29057-16.diff	16 kB	29/Oct/20 11:45 AM
backtrace.txt	2 kB	31/Aug/20 9:33 AM
security.txt	9 kB	31/Aug/20 9:33 AM

Issue Links

is a clone of

SWP-11245 You do not have permission to view this issue

Gerrit Reviews

No reviews matched the request. Check your Options in the drop-down menu of this sections header.

Activity

All | **Comments** | History | Activity | Transitions

Asterisk Team added a comment - 31/Aug/20 9:32 AM This issue has been automatically restricted and set to a blocker due to being a security type issue. If this is not a security vulnerability issue it will be moved to the appropriate issue type when triaged.

17 older comments

Friendly Automation added a comment - 05/Nov/20 2:59 PM

Change 15154 merged by Kevin Harwell:
AST-2020-001 - res_pjsip: Return dialog locked and referenced

https://gerrit.asterisk.org/c/asterisk/+/15154

Friendly Automation added a comment - 05/Nov/20 2:59 PM

Change 15155 merged by Kevin Harwell:
AST-2020-001 - res_pjsip: Return dialog locked and referenced

https://gerrit.asterisk.org/c/asterisk/+/15155

Kevin Harwell added a comment - 06/Nov/20 12:39 PM

CVE received, and docs updated:

CVE-2020-28327

I've put in a request for publication of the CVE. It might take a few days for it to sync up and be made public though.

Any further updates can't be viewed here: http://downloads.asterisk.org/pub/security/AST-2020-001.html

Sandro Gauci added a comment - 06/Nov/20 10:03 PM

Thanks for the notice. We put the CVE up on our advisory too now.

Asterisk Team added a comment - 06/Nov/20 10:03 PM

This issue has been reopened as a result of your commenting on it as the reporter. It will be triaged once again as applicable.

People

Assignee:

Kevin Harwell

Reporter:

Sandro Gauci

Issue Participants:

Asterisk Team, Friendly Automation, (3)

Issue Consultant:

Unassigned

Watchers:

5 Start watching this issue

Dates

Created:

31/Aug/20 9:32 AM

Updated:

13/Oct/21 6:14 AM

Resolved:

06/Nov/20 10:06 PM