

Details

Type: Security

Severity: Blocker

Affects Version/s: 16.17.0, 18.3.0

Components/s: Resources/res_pjsip_session

Labels: patch security

Regression: Yes

PJSIP Bundled: Yes

Status: CLOSED

Resolution: Fixed

Target Release: 16.19.1, (5)

Version/s:

Security Level: None

Description

A remote party can provoke a crash of asterisk (18.3.0, 16.17.0, master) by sending a re-INVITE after asterisk has sent a BYE (and hasn't received a response to it).

The issue was introduced in a commit fixing ~~ASTERISK-28462~~ ("res_pjsip_session: Always produce offer on re-INVITE without SDP"). The new pjsip callback added in the commit (session_inv_on_create_offer) assumes that ast_slip_session always has a channel:

```
ast_queue_unhold(session->channel);
```

When `session->channel` is `NULL`, `ast_queue_unhold(NULL)` causes Asterisk to log a few assertion failures and crash.

An example scenario is attached (config + sip + verbose console output).

Attachments		
 AST-2021-007.pdf	40 kB	30/Apr/21 8:24 AM
 AST-2021-007-16.diff	1 kB	30/Apr/21 8:24 AM
 AST-2021-007-18.diff	1 kB	30/Apr/21 8:24 AM
 extensions.conf	0.1 kB	06/Apr/21 4:40 PM
 pjsip.conf	0.1 kB	06/Apr/21 4:40 PM
 test.sh	0.1 kB	06/Apr/21 4:40 PM
 test.xml	2 kB	06/Apr/21 4:40 PM
 verbose-crash.txt	6 kB	06/Apr/21 4:40 PM

Issue Links

is a clone of

[SWP-11469](#) 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 - 06/Apr/21 4:39 PM 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. Please DO NOT put a code review up for this change at this time. Attach any


5 older comments

 Friendly Automation added a comment - 22/Jul/21 3:12 PM


Change 16202 merged by George Joseph:
AST-2021-007 - res_pjsip_session: Don't offer if no channel exists.
<https://gerrit.asterisk.org/c/asterisk/+16202>

 Friendly Automation added a comment - 22/Jul/21 3:19 PM


Change 16183 merged by Friendly Automation:
AST-2021-007 - res_pjsip_session: Don't offer if no channel exists.
<https://gerrit.asterisk.org/c/asterisk/+16183>

 Friendly Automation added a comment - 22/Jul/21 3:19 PM

Change 16182 merged by Friendly Automation:
AST-2021-007 - res_pjsip_session: Don't offer if no channel exists.
<https://gerrit.asterisk.org/c/asterisk/+16182>

 Friendly Automation added a comment - 22/Jul/21 3:19 PM

Change 16184 merged by Friendly Automation:
AST-2021-007 - res_pjsip_session: Don't offer if no channel exists.
<https://gerrit.asterisk.org/c/asterisk/+16184>

 Friendly Automation added a comment - 23/Jul/21 8:23 AM

Change 16211 merged by Friendly Automation:
AST-2021-007 - res_pjsip_session: Don't offer if no channel exists.
<https://gerrit.asterisk.org/c/asterisk/+16211>

People

Assignee:

 Joshua C. Colp

Reporter:

 Ivan Poddubny

Issue Participants:

Asterisk Team, Friendly Automation, (3)

Issue Consultant:

Unassigned

Watchers:

 Start watching this issue

Dates

Created:
06/Apr/21 4:39 PM

Updated:
14/Sep/22 10:43 AM

Resolved:
22/Jul/21 3:12 PM