Asterisk ASTERISK-29227

res_pjsip_diversion: sending multiple 181 responses causes memory corruption and crash

Details

Type:	Security	Status:	CLOSED
Severity:	Blocker	Resolution:	Fixed
Affects Version/s:	13.38.0, (7)	Target Release Version/s:	13.38.2, (6)
Component/s:	pjproject/pjsip	Security Level:	None
Labels:	patch security		
Regression:	No		
PJSIP Bundled:	Yes		

Description

Every time Asterisk/chan_pjsip transmits a "181 Call is being forwarded" packet, res_pjsip_diversion adds a "histinfo" element to Supported header. It doesn't check if "histinfo" has already been added, nor it performs a bounds check, thus making it possible to overwrite/corrupt memory past the PJSIP_GENERIC_ARRAY_MAX_COUNT elements that pjsip_supported_hdr can contain.

How to reproduce

Make a call from a pjsip endpoint to this diaplan:

```
exten => 181,1,NoOp
same => n,Set(i=9000)
same => n,While($[ ${DEC(i)} != 0])
same => n,Set(REDIRECTING(from-num)=${i})
same => n,EndWhile
```

How to crash Asterisk remotely

Use Dial application on an unanswered incoming PJSIP channel to connect to a channel indicating AST_CONTROL_REDIRECTING more than PJSIP_GENERIC_ARRAY_MAX_COUNT times (32 by default).
Example:

- 2 PJSIP endpoints [alice] and [bob]
- PJSIP/alice-00000001 executes Dial(PJSIP/bob)
- PJSIP/bob-00000002 sends an INVITE to bob
- bob sends 100 Trying, followed by repeating "181 Call Is Being Forwarded"
- Asterisk transmits 181 Call Is Being Forwarded to alice, adding one more "histinfo" element to Supported, eventually overwriting memory past array boundary until Asterisk crashes.

Attachments

0001-res_pjsip_diversion-Fix-adding-more-than-one-histinf.patch	2 kB	28/Dec/20 7:06 AM

Issue Links

is a clone of

SWP-11339 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 - 28/Dec/20 7:03 AM Thanks for creating a report! The issue has entered the triage process. That means the issue will wait in this status until a Bug Marshal has an opportunity to review the issue. Once the issue has been reviewed you will receive comments regarding the next steps towards resolut

7 older comments

Friendly Automation added a comment - 18/Feb/21 10:37 AM

Change 15466 merged by George Joseph:
res_pjsip_diversion: Fix adding more than one histinfo to Supported

https://gerrit.asterisk.org/c/asterisk/+/15466

Friendly Automation added a comment - 18/Feb/21 10:37 AM

Change 15463 merged by George Joseph:
res_pjsip_diversion: Fix adding more than one histinfo to Supported

https://gerrit.asterisk.org/c/asterisk/+/15463

Friendly Automation added a comment - 18/Feb/21 10:37 AM

Change 15454 merged by George Joseph:
res_pjsip_diversion: Fix adding more than one histinfo to Supported

https://gerrit.asterisk.org/c/asterisk/+/15454

Friendly Automation added a comment - 18/Feb/21 10:37 AM

Change 15453 merged by George Joseph:
res_pjsip_diversion: Fix adding more than one histinfo to Supported

https://gerrit.asterisk.org/c/asterisk/+/15453

Friendly Automation added a comment - 18/Feb/21 10:37 AM

Change 15451 merged by George Joseph:
res_pjsip_diversion: Fix adding more than one histinfo to Supported

https://gerrit.asterisk.org/c/asterisk/+/15451

People

Assignee:
Unassigned

Reporter:
Ivan Poddubny

Issue Participants:
Asterisk Team, Friendly Automation, (2)

Issue Consultant:
Unassigned

Watchers:
4 Start watching this issue

Dates

Created:
28/Dec/20 7:03 AM

Updated:
13/Oct/21 6:10 AM

Resolved:
18/Feb/21 10:37 AM