Crash in receiving updated SDP answer after initial SDP negotiation failed

Moderate **sauwming** published **GHSA-hvq6-f89p-frvp** on Mar 8, 2021

Package

No package listed

Affected versions

2.10 or lower

Patched versions

2.11

Description

After an initial INVITE has been sent, when two 183 responses are received, with the first one causing negotiation failure, a crash will occur:

```
#0  0x00007fb40787f5bd in pj_strdup (pool=0x7fb37453c490, dst=0x7fb378140b18, src=0x0) at ../include/pj/string_i.h:40
#1  0x00007fb40782806c in pjmedia_sdp_neg_modify_local_offer2 (pool=0x7fb37453c490, neg=0x7fb3682f0f30, flags=1, local=0x7fb3680d1fb8)
    at ../src/pjmedia/sdp_neg.c:336
#2  0x00007fb4077a1d9e in inv_check_sdp_in_incoming_msg (inv=0x7fb3682f0c68, tsx=0x7fb3a8154208, rdata=0x7fb38832d3b8)
    at ../src/pjsip-ua/sip_inv.c:2084
#3  0x00007fb4077a5bbd in inv_on_state_early (inv=0x7fb3682f0c68, e=0x7fb2f4ad7a70) at ../src/pjsip-ua/sip_inv.c:4447
#4  0x00007fb40779f4a3 in mod_inv_on_tsx_state (tsx=0x7fb3a8154208, e=0x7fb2f4ad7a70) at ../src/pjsip-ua/sip_inv.c:736
#5  0x00007fb4077ec047 in pjsip_dlg_on_tsx_state (dlg=0x7fb3960c48a8, tsx=0x7fb3a8154208, e=0x7fb2f4ad7a70) at ../src/pjsip/sip_dialog.c:2129
#6  0x00007fb4077ec8b9 in mod_ua_on_tsx_state (tsx=0x7fb3a8154208, e=0x7fb2f4ad7a70) at ../src/pjsip/sip_ua_layer.c:178
```

Impact

The vulnerability causes PJSIP to crash, resulting in a denial of service.

Patches

A patch in commit `97b3d7a` has been merged into master.

For more information

If you have any questions or comments about this advisory:

- Email us at contact@pjsip.org

Severity

Moderate

CVE ID

CVE-2021-21375

Weaknesses

No CWEs