pjsip / **pjproject** Public

Code | Issues 3 | Pull requests 3 | Actions | Security and quality 39 | In

Commit 4225a93

sauwming authored on Mar 10 · 44 / 45 · Verified

Fixed SIP Multipart CID URI length check (#4844)

1 parent 450f838 commit 4225a93

1 file changed +3 -1

Top

Filter files...

pjsip/src/pjsip

sip_multipart.c

Search within code

pjsip/src/pjsip/sip_multipart.c

```
@@ -549,12 +549,14 @@ static pj_str_t cid_uri_to_hdr_value(pj_pool_t *pool,
pj_str_t *cid_uri)
549 549     pj_size_t cid_len = pj_strlen(cid_uri);
550 550     pj_size_t alloc_len = cid_len + 2 /* for the leading and trailing angle
        brackets */;
551 551     pj_str_t uri_overlay;
552       -     pj_str_t cid_hdr;
      552 +     pj_str_t cid_hdr = {0};
553 553     pj_str_t hdr_overlay;
554 554
555 555     pj_strassign(&uri_overlay, cid_uri);
556 556     /* If the URI is already enclosed in angle brackets, remove them. */
```

```
557  557        if (uri_overlay.ptr[0] == '<') {
     558  +         if (uri_overlay.slen < 2)
     559  +             return cid_hdr;
558  560            uri_overlay.ptr++;
559  561            uri_overlay.slen -= 2;
560  562        }
```

Comments 0