MPD: FreeBSD PPP daemon Bugs

FreeBSD Multi PPP daemon

Brought to you by: amotin, dadv, dmitryluhtionov

#70 report an another vulnerability

Milestone: None **Status:** closed-fixed **Owner:** Eugene Grosbein **Labels:** None
Priority: 5
Updated: 2020-09-07 **Created:** 2020-09-04 **Creator:** chennan **Private:** No

Hello,
I find an another memory corruption vulnerability in l2tp protocol.
The vulnerability is in the 'ppp_l2tp_avp_list2ptrs' function of the l2tp_avp.c file, which has the following code:

```
case AVP_CAUSE_CODE:
    AVP_ALLOC(causecode);
    ptrs->causecode->causecode = ntohs(ptr16[0]);
    ptrs->causecode->causemsg = ptr8[3];
    memcpy(ptrs->causecode->message,
        (char *)avp->value + 3, avp->vlen - 3);
    break;
```

There is no check here whether 'avp->vlen' is less than 3. This will lead to OOW.

Discussion

Eugene Grosbein - *2020-09-04*
Thank you for the report. The issue is being investigated, please wait.

Eugene Grosbein - *2020-09-06*
Thank you very much for your patience. The problem is confirmed and fixed. New version 5.9 containing the fix is released.

chennan - *2020-09-06*
May I apply for a CVE number?

Eugene Grosbein - *2020-09-06*
Sure.

Eugene Grosbein - *2020-09-06*
- **status**: open --> closed-fixed
- **private**: Yes --> No
- **Group**: -->

Xin LI - *2020-09-07*
We (FreeBSD security team) have assigned CVE-2020-7465 for this one (I'm posting this here mainly to avoid duplicated allocations).

chennan - *2020-09-07*
Thank you very much.
Discoverer(s): ChenNan Of Chaitin Security Research Lab

Log in to post a comment.

Company

About
Team
SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support
Site Documentation
Site Status