MPD: FreeBSD PPP daemon Bugs

FreeBSD Multi PPP daemon

Brought to you by: amotin, dadv, dmitryluhtionov

#69 report a vulnerability

Milestone: None **Status:** closed-fixed **Owner:** Eugene Grosbein **Labels:** None
Priority: 5
Updated: 2020-09-07 **Created:** 2020-09-03 **Creator:** chennan **Private:** No

Hello,
I find a memory corruption vulnerability in ppp protocol.
The vulnerability is in the AuthInput function of the auth.c file, which has the following code:

```
bp = mbread(bp, &fsmh, sizeof(fsmh));
if (len > ntohs(fsmh.length))
    len = ntohs(fsmh.length);
len -= sizeof(fsmh);
   // If fsmh.length is less than sizeof(fsmh), then the 'len'  will  overflow.
```

There is no check here whether 'fsmh.length' is less than 'sizeof(fsmh)'.

After 'len' reaches an overflow, code execute to the EapInput->EapRadiusProxy function.

In the EapRadiusProxy function, there are the following lines of code:

```
  auth->params.eapmsg = Malloc(MB_AUTH, len + sizeof(lh));
                  //len + sizeof(lh)  integer overflow
  memcpy(auth->params.eapmsg, &lh, sizeof(lh));
  memcpy(&auth->params.eapmsg[sizeof(lh)], pkt, len);
               //buffer overflow
```

len + sizeof(lh) will integer overflow again.
Caused to allocate a length of insufficient buffer, and then memcpy caused buffer overflow.

Discussion

Eugene Grosbein - *2020-09-03*

Thank you very much for the report. The fix will be ready soon.

chennan - *2020-09-03*

You are welcome. May I apply for a cve number?

Eugene Grosbein - *2020-09-03*

I believe this problem is not exploitable.

Eugene Grosbein - *2020-09-03*

The fix committed as https://sourceforge.net/p/mpd/svn/2374/

Note that "len + sizeof(lh)" will not overflow again: "len" is of u_short type and sizeof() is of unsigned int type, so "len" is promoted to unsigned int before addition.

sizeof(fsmh) equals to 4 bytes, so the problem could occur when fsmh.length is less than 4 in which case len would be more than 65532 after initial overflow. Unsigned integer has at least 32 bits for any FreeBSD supported architecture, so this would result in Malloc'ing slightly over 64KB.

chennan - *2020-09-04*

Well, you are right, I will continue to find if it can be converted to memory corruption.

chennan - *2020-09-06*

Sorry to disturb you again. Even though this vulnerability can't be OOW, but it can be OOR. At least it is a remote unauthorized DOS, which is still dangerous. Is it right?

Eugene Grosbein - *2020-09-06*

Probably, yes. Anyway, it is fixed already.

Eugene Grosbein - *2020-09-04*

- **status**: open --> closed-fixed
- **private**: Yes --> No
- **Group**: -->

Xin LI - *2020-09-07*

Please use CVE-2020-7466.

chennan - *2020-09-07*

Thank you very much.
Discoverer(s): ChenNan Of Chaitin Security Research Lab

Log in a comment.