New issue

Jump to bottom

sprintf() trigger buffer overflow on `do_retr()` function #2

⊙ Open **H4niz** opened this issue on Aug 24, 2021 · 0 comments

H4niz commented on Aug 24, 2021

Hi **@Gabe-commiter**,
I found a issue, that can trigger buffer overflow on your application. The issue exists on `do_retr()` function (from line 706 to 791) on ftpproto.c

At glance, we can see you defined `char arg[MAX_ARG];` , it's not problem, however, when you use `sprintf()` on line 718 and 721, they trigger bufferoverflow.

```
typedef struct session
{
/*
        Defined on common.h
                #define MAX_COMMAND_LINE 1024
                #define MAX_COMMAND 32
                #define MAX_ARG     1024

                #define MAX_BUFFER_SIZE 1024
*/

#define MAX_BUFFER_SIZE 1024
        uid_t    uid;
        int ctrl_fd;//¿ØÖÆÃèÊö·û
        char cmdline[MAX_COMMAND_LINE];
        char cmd[MAX_COMMAND];
        char arg[MAX_ARG];
....
        <truncated>
....
}session_t;



static void do_retr(session_t *sess)
{
        <truncated>
....
        char buf[MAX_BUFFER_SIZE] = {0}; // Defined buffer called buf with MAX_BUFFER_SIZE length
        //2ÅÐ¶Ï´«ÊäÄ£Ê½
        if(sess->is_ascii)
// trigger the buffer overflow because length of sess->arg is defined 1024 length,
// in order that, when sprintf is executed, the buffer `buf` can be write total  len("Opening ASCII mode data connection for ") + MAX_BUFFER_SIZE + len(" (%ld bytes)")
                sprintf(buf,  "Opening ASCII mode data connection for %s (%ld bytes)", sess->arg, sbuf.st_size);//Ascii
        else
// trigger the buffer overflow because length of sess->arg is defined 1024 length,
// in order that, when sprintf is executed, the buffer `buf` can be write total  len("Opening ASCII mode data connection for ") + MAX_BUFFER_SIZE + len(" (%ld bytes)")
                sprintf(buf, "Opening BINARY mode data connection for %s (%ld bytes)", sess->arg, sbuf.st_size);
...
        <truncated>
...
}
```

Solution: Please use `snprintf()` to limit maximum input characters.
See: https://www.geeksforgeeks.org/snprintf-c-library/

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant