New issue

Jump to bottom

Buffer overflows problem #1

Open **ghost** opened this issue on Aug 22, 2021 · 1 comment

ghost commented on Aug 22, 2021

Buffer overflow exists in the `do_mkd` function in the `ftpproto.c` file. Overwrite rbp when new path name length exceeds 1032.

```
#define MAX_BUFFER_SIZE 1024        //it defined in common.h

char buf[MAX_BUFFER_SIZE] = {0};    //buf[1024]={0}
sprintf(buf, "\"%s/%s\" created",buf,sess->arg);
```

H4niz commented on Aug 24, 2021

Hi **@Gabe-commiter**,
To fix this issue, you can you `snprintf()` instead of `sprintf()` to limit maximun bytes that are read into buffer. For detail:

```
int snprintf(char *str, size_t size, const char *format, ...);

*str : is a buffer.
size : is the maximum number of bytes
(characters) that will be written to the buffer.
format : C string that contains a format
string that follows the same specifications as format in printf
... : the optional ( …) arguments
are just the string formats like (“%d”, myint) as seen in printf.
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant