

0

Reported on Jan 23rd 2022

Stack Pointer (\$RSP) is corrupted at function eval7t in eval.c during calling eval3, eval4, eval5, eval6, eval7... continuously while parsing too many brackets.

latest commit hash : 79a6e25b79cdb35e00d8b364516103eb358d8cc7

[illegible]

Chat with us

Chat with us

[illegible]

[illegible]

```
$ ./vim -u ./poc
```

Chat with us

```
-----  
  
times>...)  
  
0x28],rax)  
  
times>...)  
times>...)  
JPT direction over  
-----  
  
28  
],rax  
  
l7t+54>  
  
-----  
  
-----  
  
7f5666661870
```

Chat with us

```

-----

times>...)

0x28],rax)

times>...)
times>...)
JPT direction over
-----

28
],rax

17t+54>

-----
-----

7f5555551070

```

```

-----

times>...)

0x28],rax)

times>...)
times>...)
JPT direction over
-----

28
],rax

17t+54>

-----
-----

7f5555551070

```

`gdb-peda$ exploitable`

Description: Possible stack corruption

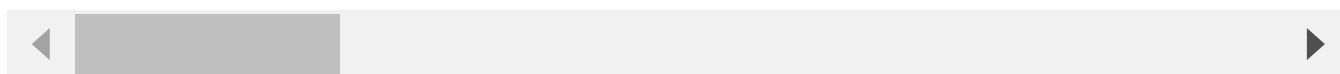
Short description: PossibleStackCorruption (7/22)

Hash: 4d4a9714ed5fc41d3e60eba892fbac67.ffa116d70a8fd39d0c6006916f349ae57

Exploitability Classification: EXPLOITABLE

Explanation: GDB generated an error while unwinding the stack and/or the si

Other tags: DestAv (8/22), AccessViolation (21/22)



Impact

This vulnerability may lead to an exploit of this program since this bug can corrupt \$RSP register. This kind of memory corruption vulnerabilities can cause bypass protection mechanisms and be successful arbitrary code execution.

Acknowledgement

Special thanks to Pocas (a.k.a Kapos)

CVE

CVE-2022-0351

(Published)

Vulnerability Type

CWE-786: Access of Memory Location Before Start of Buffer

Severity

High (8.4)

Visibility

Public

Status

Fixed

Found by



alkyne Choi

@alkyne

unranked ▼

Chat with us

Fixed by



Bram Moolenaar

@brammool

maintainer

This report was seen 989 times.

We are processing your report and will contact the **vim** team within 24 hours. 10 months ago

alkyne Choi modified the report 10 months ago

alkyne Choi modified the report 10 months ago

alkyne Choi modified the report 10 months ago

We have contacted a member of the **vim** team and are waiting to hear back 10 months ago

Bram Moolenaar validated this vulnerability 10 months ago

alkyne Choi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago

It simply runs out of stack. I limit the depth to 1000 in patch 8.2.4206.

Bram Moolenaar marked this as fixed in **8.2** with commit **fe6fb2** 10 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Pocas 10 months ago

I am not Kapos,, but nice this. (Just legend)

Chat with us



Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

Chat with us