php.net | support | documentation | report a bug | advanced search | search howto | statistics | random bug | login

go to bug id or search bugs for

Sec Bug #81723 Heap buffer overflow in finfo_buffer

Submitted:	2022-06-27 22:59 UTC	**Modified:**	2022-07-05 07:05 UTC
From:	xd4rker at gmail dot com	**Assigned:**	stas (profile)
Status:	Closed	**Package:**	Filesystem function related
PHP Version:	8.1.7	**OS:**	Linux
Private report:	No	**CVE-ID:**	2022-31627

View **Add Comment** **Developer** **Edit**

[2022-06-27 22:59 UTC] xd4rker at gmail dot com

```
Description:
------------
The following content is causing a heap-based buffer overflow in finfo_buffer. This was found using AFL++.

00000000  00 01 8a 75 70 00 10 97  db 97 97 98 97 97 7d 87  |...up.........}.|
00000010  97 97 97 00 00 92 00 1f  00 51 00 00 00 00 00 00  |.........Q......|
00000020  00 00 00 ff ff 7f ff 00  00 00 00 00 1e 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 0c 00 00 00 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  dc 00 00 00 01 00 00 00  |................|
00000050  00 00 00 00 00 4f 01 19  00 00 7f 00 00 00 00 00  |.....O..........|
00000060  18 00 39 00 00 00 00 00  00 00 00 00 00 00 00 00  |..9.............|
00000070  00 00 dc 00 00 00 01 00  00 00 00 00 00 00 00 4f  |...............O|
00000080  01 19 00 00 7f 00 00 f5  00 00 00 00 ee ff 00 00  |................|
00000090  00 00 00 00 00 00 01 00  00 fd 00                 |...........|

Tested against PHP >= 8.1.

ASAN output:

==4777==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60e000000000 at pc 0x000000faba20 bp 0x7ffc087ab460
sp 0x7ffc087ab458
READ of size 8 at 0x60e000000000 thread T0
    #0 0xfaba1f in zend_mm_realloc_heap /home/user/php-src/Zend/zend_alloc.c:1561:3
    #1 0xfaba1f in _erealloc /home/user/php-src/Zend/zend_alloc.c:2582:9
    #2 0xa94368 in file_check_mem /home/user/php-src/ext/fileinfo/libmagic/funcs.c:623:14
    #3 0xa9f566 in match /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:458:9
    #4 0xaa2748 in file_softmagic /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:138:13
    #5 0xaa2748 in mget /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:1836:8
    #6 0xa9f04c in match /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:360:12
    #7 0xaa49b2 in mget /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:1885:8
    #8 0xa9f04c in match /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:360:12
    #9 0xa9e37e in file_softmagic /home/user/php-src/ext/fileinfo/libmagic/softmagic.c:138:13
    #10 0xa93762 in file_buffer /home/user/php-src/ext/fileinfo/libmagic/funcs.c:459:7
    #11 0xa98c42 in magic_buffer /home/user/php-src/ext/fileinfo/libmagic/magic.c:273:6
    #12 0xa6eb87 in _php_finfo_get_type /home/user/php-src/ext/fileinfo/fileinfo.c:346:23
    #13 0x12947cd in ZEND_DO_ICALL_SPEC_RETVAL_UNUSED_HANDLER /home/user/php-src/Zend/zend_vm_execute.h:1250:2
    #14 0x114f0a9 in execute_ex /home/user/php-src/Zend/zend_vm_execute.h:55687:7
    #15 0x114f93c in zend_execute /home/user/php-src/Zend/zend_vm_execute.h:60251:2
    #16 0x1071860 in zend_eval_stringl /home/user/php-src/Zend/zend_execute_API.c:1271:4
    #17 0x1071e15 in zend_eval_stringl_ex /home/user/php-src/Zend/zend_execute_API.c:1313:11
    #18 0x1071e15 in zend_eval_string_ex /home/user/php-src/Zend/zend_execute_API.c:1323:9
    #19 0x153f8ff in do_cli /home/user/php-src/sapi/cli/php_cli.c:998:5
    #20 0x153dae0 in main /home/user/php-src/sapi/cli/php_cli.c:1336:18
    #21 0x7f612802e082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
    #22 0x602b6d in _start (/home/user/php-src-8.1/sapi/cli/php+0x602b6d)

0x60e000000000 is located 64 bytes to the left of 154-byte region [0x60e000000040,0x60e0000000da)
allocated by thread T0 here:
    #0 0x667654 in strdup (/home/user/php-src-8.1/sapi/cli/php+0x667654)
    #1 0x15595a7 in save_ps_args /home/user/php-src/sapi/cli/ps_title.c:195:30

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/user/php-src/Zend/zend_alloc.c:1561:3 in zend_mm_realloc_heap
Shadow bytes around the buggy address:
  0x0c1c7fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c1c7fff8000:[fa]fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c1c7fff8010: 00 00 00 00 00 00 00 00 00 00 00 02 fa fa fa fa
  0x0c1c7fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa
  0x0c1c7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff8050: 00 00 00 00 fa fa fa fa fa fa fa fa 00 00 00 00
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
==4777==ABORTING

Test script:
---------------
<?php

$data =
hex2bin("00018a7570001097db97979897977d87979797000092001f0051000000000000000000ffff7fff00000000001e0000000000000000000000000c0000000000000000000000000000c


$f = finfo_open();
finfo_buffer($f, $data);

Expected result:
----------------
MacBinary, total length 256, Mon Feb  6 06:28:16 2040 INVALID date, modified Fri Feb 24 11:23:37 2040, creator '    ',
20225 bytes "\212" , at 0x4f81 419430527 bytes resource

Actual result:
--------------
zend_mm_heap corrupted
```

Patches

Add a Patch

Pull Requests

Add a Pull Request

History

All Comments Changes Git/SVN commits Related reports

[2022-06-28 15:13 UTC] cmb@php.net

```
-Package: *Graphics related
+Package: Filesystem function related
-Assigned To:
+Assigned To: cmb
```

[2022-06-28 15:13 UTC] cmb@php.net

I can confirm the memory corruption, but that looks like a
libmagic issue (which may have been fixed in the meantime).

[2022-06-30 14:54 UTC] cmb@php.net

```
-Status: Assigned
+Status: Analyzed
```

[2022-06-30 14:54 UTC] cmb@php.net

No, this is not an upstream issue, but rather caused by a bad
patch of libmagic 5.40 and affects PHP-8.1+; we try to
`erealloc()` memory which has been `malloc()`d.

[2022-06-30 15:32 UTC] cmb@php.net

```
Proposed patch: <https://gist.github.com/cmb69/90aba3c8ff8d42c5598e31846d259aa7>.
This includes updates to libmagic.patch, created by running ./generate_patch.sh.

Stas, can you please handle this?
```

[2022-06-30 15:37 UTC] cmb@php.net

```
-Assigned To: cmb
+Assigned To: stas
```

[2022-06-30 22:13 UTC] stas@php.net

```
-CVE-ID:
+CVE-ID: needed
```

[2022-07-05 06:37 UTC] stas@php.net

```
-CVE-ID: needed
+CVE-ID: 2022-31627
```

[2022-07-05 07:05 UTC] git@php.net

```
Automatic comment on behalf of cmb69 (author) and smalyshev (committer)
Revision: https://github.com/php/php-src/commit/ca6d511fa54b34d5b75bf120a86482a1b9e1e686
Log: Fix #81723: Memory corruption in finfo_buffer()
```

[2022-07-05 07:05 UTC] git@php.net

```
-Status: Analyzed
+Status: Closed
```

Last updated: Sat Nov 26 03:05:54 2022 UTC