Sec Bug #79171 heap-buffer-overflow in phar_extract_file

Submitted: 2020-01-26 15:03 UTC **Modified:** 2020-02-17 08:23 UTC
From: cmb@php.net **Assigned:** stas (profile)
Status: Closed **Package:** PHAR related
PHP Version: 7.3Git-2020-01-26 (Git) **OS:** Windows
Private report: No **CVE-ID:** 2020-7061

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

[2020-01-26 15:03 UTC] cmb@php.net

```
Description:
------------
As of PHP 7.3.0, basically whenever phar_extract_file() is called
on Windows, there is a heap buffer overflow caused by an incorrect
loop termination.  Several phar tests exhibit the issue when run
with ASan enabled.



Test script:
---------------
php run-tests.php --asan ext\phar\tests\bug70019.phpt

Actual result:
--------------
=================================================================
==6228==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x11d87801af45 at pc 0x7ff8a01de4e7 bp 0x003ef9ffa080
sp 0x003ef9ffa0c8
READ of size 1 at 0x11d87801af45 thread T0
    #0 0x7ff8a01de4e6 in phar_extract_file C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4173
    #1 0x7ff8a01a71a0 in extract_helper C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4317
    #2 0x7ff8a01a6591 in zim_Phar_extractTo C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4441
    #3 0x7ff89d7eceb9 in ZEND_DO_FCALL_SPEC_RETVAL_UNUSED_HANDLER C:\php-sdk\phpdev\vc15\x64\php-src-
7.4\Zend\zend_vm_execute.h:1618
    #4 0x7ff89d4f9560 in execute_ex C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_vm_execute.h:53611
    #5 0x7ff89d4fb006 in zend_execute C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_vm_execute.h:57913
    #6 0x7ff89d173dc2 in zend_execute_scripts C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend.c:1665
    #7 0x7ff89e3212fb in php_execute_script C:\php-sdk\phpdev\vc15\x64\php-src-7.4\main\main.c:2617
    #8 0x7ff6fe7394db in do_cli C:\php-sdk\phpdev\vc15\x64\php-src-7.4\sapi\cli\php_cli.c:961
    #9 0x7ff6fe734675 in main C:\php-sdk\phpdev\vc15\x64\php-src-7.4\sapi\cli\php_cli.c:1352
    #10 0x7ff6fe7a2e33 in __scrt_common_main_seh
d:\agent\_work\2\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #11 0x7ff8f5a57bd3  (C:\WINDOWS\System32\KERNEL32.DLL+0x180017bd3)
    #12 0x7ff8f6dcced0  (C:\WINDOWS\SYSTEM32\ntdll.dll+0x18006ced0)

0x11d87801af45 is located 0 bytes to the right of 21-byte region [0x11d87801af30,0x11d87801af45)
allocated by thread T0 here:
    #0 0x7ff8b7544e1b  (C:\Program Files\LLVM\lib\clang\9.0.0\lib\windows\clang_rt.asan_dynamic-
x86_64.dll+0x180034e1b)
    #1 0x7ff89d2654dd in __zend_realloc C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_alloc.c:2994
    #2 0x7ff89d27aa01 in tracked_realloc C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_alloc.c:2716
    #3 0x7ff89d264784 in _realloc_custom C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_alloc.c:2434
    #4 0x7ff89d2642a6 in _erealloc C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_alloc.c:2556
    #5 0x7ff89e219895 in virtual_file_ex C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_virtual_cwd.c:1146
    #6 0x7ff8a01ddd76 in phar_extract_file C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4153
    #7 0x7ff8a01a71a0 in extract_helper C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4317
    #8 0x7ff8a01a6591 in zim_Phar_extractTo C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4441
    #9 0x7ff89d7eceb9 in ZEND_DO_FCALL_SPEC_RETVAL_UNUSED_HANDLER C:\php-sdk\phpdev\vc15\x64\php-src-
7.4\Zend\zend_vm_execute.h:1618
    #10 0x7ff89d4f9560 in execute_ex C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_vm_execute.h:53611
    #11 0x7ff89d4fb006 in zend_execute C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend_vm_execute.h:57913
    #12 0x7ff89d173dc2 in zend_execute_scripts C:\php-sdk\phpdev\vc15\x64\php-src-7.4\Zend\zend.c:1665
    #13 0x7ff89e3212fb in php_execute_script C:\php-sdk\phpdev\vc15\x64\php-src-7.4\main\main.c:2617
    #14 0x7ff6fe7394db in do_cli C:\php-sdk\phpdev\vc15\x64\php-src-7.4\sapi\cli\php_cli.c:961
    #15 0x7ff6fe734675 in main C:\php-sdk\phpdev\vc15\x64\php-src-7.4\sapi\cli\php_cli.c:1352
    #16 0x7ff6fe7a2e33 in __scrt_common_main_seh
d:\agent\_work\2\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #17 0x7ff8f5a57bd3  (C:\WINDOWS\System32\KERNEL32.DLL+0x180017bd3)
    #18 0x7ff8f6dcced0  (C:\WINDOWS\SYSTEM32\ntdll.dll+0x18006ced0)

SUMMARY: AddressSanitizer: heap-buffer-overflow C:\php-sdk\phpdev\vc15\x64\php-src-7.4\ext\phar\phar_object.c:4173 in
phar_extract_file
Shadow bytes around the buggy address:
  0x040d86f83590: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x040d86f835a0: fd fd fa fa fd fd fd fd fa fa 00 00 00 fa fa fa
  0x040d86f835b0: 00 00 07 fa fa fa 00 00 00 00 fa fa fd fd fd fd
  0x040d86f835c0: fa fa fd fd fd fd fa fa 00 00 00 00 fa fa 00 00
  0x040d86f835d0: 00 fa fa fa 00 00 00 00 fa fa 00 00 00 fa fa fa
=>0x040d86f835e0: fd fd fd fa fa fa 00 00[05]fa fa fa fa fa fa fa
  0x040d86f835f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x040d86f83600: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x040d86f83610: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x040d86f83620: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x040d86f83630: 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
==6228==ABORTING
```

Patches

Add a Patch

Pull Requests

Add a Pull Request

History

All | Comments | Changes | Git/SVN commits | Related reports

[2020-01-26 15:04 UTC] cmb@php.net

```
-Status: Open
+Status: Assigned
-Assigned To:
+Assigned To: stas
```

[2020-01-26 15:04 UTC] cmb@php.net

```
Suggested patch:
<https://gist.github.com/cmb69/3f86d1947dacca958374323997c45d63>.
```

[2020-02-09 23:06 UTC] stas@php.net

```
-CVE-ID:
+CVE-ID: 2020-7061
```

[2020-02-10 03:54 UTC] stas@php.net

```
Added to security repo as e0a0856089bee6aaf6a19b476a0eb552a4319a5f.
```

[2020-02-17 08:23 UTC] stas@php.net

```
-Status: Assigned
+Status: Closed
```

[2020-02-17 08:23 UTC] stas@php.net

```
The fix for this bug has been committed.
If you are still experiencing this bug, try to check out latest source from https://github.com/php/php-src and re-test.
Thank you for the report, and for helping us make PHP better.
```