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 #79282 Use-of-uninitialized-value in exif

Submitted:	2020-02-19 09:31 UTC	**Modified:**	2020-03-17 05:39 UTC
From:	nikic@php.net	**Assigned:**	stas (profile)
Status:	Closed	**Package:**	EXIF related
PHP Version:	master-Git-2020-02-19 (Git)	**OS:**	
Private report:	No	**CVE-ID:**	2020-7064

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

[2020-02-19 09:31 UTC] nikic@php.net

```
Description:
------------
From https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=19581.

<?php
var_dump(exif_read_data('data://image/jpeg;base64,/9jhAAlFeGlmAAAg'));

Results in:

        Uninitialized bytes in MemcmpInterceptorCommon at offset 1 inside [0x7010000006e8, 2)
        ==1==WARNING: MemorySanitizer: use-of-uninitialized-value
            #0 0x5004dc in __interceptor_bcmp /src/llvm-project/compiler-
rt/lib/sanitizer_common/sanitizer_common_interceptors.inc:885:10
            #1 0x86693b in exif_process_TIFF_in_JPEG php-src/ext/exif/exif.c:3596:6
            #2 0x861b7e in exif_scan_JPEG_header php-src/ext/exif/exif.c:3793:6
            #3 0x8609eb in exif_scan_FILE_header php-src/ext/exif/exif.c:4186:8
            #4 0x8602bb in exif_read_from_impl php-src/ext/exif/exif.c:4327:8
            #5 0x858b52 in exif_read_from_stream php-src/ext/exif/exif.c:4344:8
            #6 0x856001 in zif_exif_read_data php-src/ext/exif/exif.c:4434:9
            #7 0x112596d in zend_call_function php-src/Zend/zend_execute_API.c:817:4
            #8 0x11236e2 in _call_user_function_ex php-src/Zend/zend_execute_API.c:638:9
            #9 0x1696c7a in fuzzer_call_php_func_zval php-src/sapi/fuzzer/fuzzer-sapi.c:247:2
            #10 0x169596f in LLVMFuzzerTestOneInput php-src/sapi/fuzzer/fuzzer-exif.c:52:2
            #11 0x481101 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerLoop.cpp:556:15
            #12 0x46bc21 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:292:6
            #13 0x4718de in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long))
/src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:774:9
            #14 0x49b802 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:19:10
            #15 0x7f3e6199882f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/libc-start.c:291
            #16 0x445098 in _start

          Uninitialized value was created by a heap allocation
            #0 0x4fc67d in malloc /src/llvm-project/compiler-rt/lib/msan/msan_interceptors.cpp:925:3
            #1 0x1088155 in __zend_malloc php-src/Zend/zend_alloc.c:2975:14
            #2 0x1082159 in _emalloc php-src/Zend/zend_alloc.c:2535:10
            #3 0x865d76 in exif_file_sections_add php-src/ext/exif/exif.c:2042:10
            #4 0x8618c0 in exif_scan_JPEG_header php-src/ext/exif/exif.c:3747:8
            #5 0x8609eb in exif_scan_FILE_header php-src/ext/exif/exif.c:4186:8
            #6 0x8602bb in exif_read_from_impl php-src/ext/exif/exif.c:4327:8
            #7 0x858b52 in exif_read_from_stream php-src/ext/exif/exif.c:4344:8
            #8 0x856001 in zif_exif_read_data php-src/ext/exif/exif.c:4434:9
            #9 0x112596d in zend_call_function php-src/Zend/zend_execute_API.c:817:4
            #10 0x11236e2 in _call_user_function_ex php-src/Zend/zend_execute_API.c:638:9
            #11 0x1696c7a in fuzzer_call_php_func_zval php-src/sapi/fuzzer/fuzzer-sapi.c:247:2
            #12 0x169596f in LLVMFuzzerTestOneInput php-src/sapi/fuzzer/fuzzer-exif.c:52:2
            #13 0x481101 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerLoop.cpp:556:15
            #14 0x46bc21 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:292:6
            #15 0x4718de in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long))
/src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:774:9
            #16 0x49b802 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:19:10
            #17 0x7f3e6199882f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/libc-start.c:291

I can't reproduce under valgrind, so also can't tell which versions are affected.
```

Patches

Add a Patch

Pull Requests

Add a Pull Request

History

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

[2020-02-19 10:08 UTC] nikic@php.net

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

[2020-02-19 10:08 UTC] nikic@php.net

```
Patch candidate: https://gist.github.com/nikic/041b154eb0919e1d407523eca9b21176

This is really a one byte out-of-bounds read that happens to fall into one uninitialized byte that was over-allocated.
I'm adding a bounds check and removing the over-allocation.
```

[2020-02-24 18:12 UTC] stas@php.net

```
-CVE-ID:
```

```
+CVE-ID: 2020-7064
```

[2020-03-16 03:30 UTC] stas@php.net

```
I've verified that the fix fixes the issue on oss-fuzz setup.
```

[2020-03-17 05:39 UTC] stas@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=41f66e2a2cfd611e35be5ac3bf747f0b56161216
Log: Fixed bug #79282
```

[2020-03-17 05:39 UTC] stas@php.net

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

[2020-03-17 05:40 UTC] stas@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=25238bdf6005b85ab844aa2b743b589dfce9f0d2
Log: Fixed bug #79282
```

[2020-03-17 05:41 UTC] stas@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=b9d32197cb96879ee7b4bee835b68a7eb780ca36
Log: Fixed bug #79282
```

[2020-03-17 05:43 UTC] stas@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=9ed82b1f7b17bf505fa22944185631e3e8156cf0
Log: Fixed bug #79282
```

[2020-03-17 08:30 UTC] cmb@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=c099c71ea5c25cf6b435cbf288e35403c49c17a6
Log: Fixed bug #79282
```

[2020-03-17 09:48 UTC] cmb@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=25238bdf6005b85ab844aa2b743b589dfce9f0d2
Log: Fixed bug #79282
```

[2020-03-17 09:48 UTC] cmb@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=b9d32197cb96879ee7b4bee835b68a7eb780ca36
Log: Fixed bug #79282
```

[2020-03-17 10:02 UTC] cmb@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=41f66e2a2cfd611e35be5ac3bf747f0b56161216
Log: Fixed bug #79282
```

[2020-03-17 10:22 UTC] derick@php.net

```
Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=0c77b4307df73217283a4aaf9313e1a33a0967ff
Log: Fixed bug #79282
```

Last updated: Mon Dec 19 01:05:54 2022 UTC