## Sec Bug #81708 UAF due to php_filter_float() failing for ints

| | | | |
|---|---|---|---|
| **Submitted:** | 2022-01-30 09:00 UTC | **Modified:** | 2022-02-14 06:07 UTC |
| **From:** | dukk at softdev dot online | **Assigned:** | stas (profile) |
| **Status:** | Closed | **Package:** | Filter related |
| **PHP Version:** | 8.0.15 | **OS:** | centos 8 |
| **Private report:** | No | **CVE-ID:** | 2021-21708 |

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

**[2022-01-30 09:00 UTC] dukk at softdev dot online**

```
Description:
------------
NGINX + php-fpm (versions tested 7.4.27, 8.0.15):
1. place files from URL in webserver directory
2. Requires PostgreSQL valid (nonce) connection string (edit B.php)
3. make request (curl "http://127.0.0.1/A.php")
4. obtain HTTP 502 in client and php-fpm process on server

in A.php change xml attribute val to "+11."  - all if fine. no crash.


this PoC is extracted (stripped-down) from large code-base.

Test script:
---------------
https://github.com/MrdUkk/php-sigsegv

Expected result:
----------------
expected result is seening
PHP Fatal error:  Uncaught Error: Class "APIException" not found in A.php:27


Actual result:
--------------
HTTP 502 and php-fpm server process crashed

Program received signal SIGSEGV, Segmentation fault.
0x000055ba505e7295 in _emalloc ()
(gdb) bt
#0  0x000055ba505e7295 in _emalloc ()
#1  0x000055ba505e810f in _ecalloc ()
#2  0x000055ba504a4977 in timelib_get_time_zone_info ()
#3  0x000055ba504a6a7f in timelib_unixtime2local ()
#4  0x000055ba50480c41 in php_format_date ()
#5  0x000055ba504572bc in php_log_err_with_severity ()
#6  0x000055ba5045771a in php_error_cb ()
#7  0x000055ba5045c3aa in zend_error_va_list ()
#8  0x000055ba5045c991 in zend_error ()
#9  0x000055ba5045833b in php_verror ()
#10 0x000055ba5045845c in php_error_docref ()
#11 0x00007f641246afd4 in pdo_raise_impl_error.cold () from target:/usr/lib64/php/modules/pdo.so
#12 0x00007f6412471e72 in zim_PDOStatement_bindValue () from target:/usr/lib64/php/modules/pdo.so
#13 0x000055ba50695a50 in execute_ex ()
#14 0x000055ba50696861 in zend_execute ()
#15 0x000055ba5060d2db in zend_execute_scripts ()
#16 0x000055ba505aa488 in php_execute_script ()
#17 0x000055ba50476af9 in main ()
(gdb)
```

## Patches

Add a Patch

## Pull Requests

Add a Pull Request

## History

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

**[2022-01-31 14:47 UTC] cmb@php.net**

```
-Summary: PHP-FPM sigsegv
+Summary: UAF due to php_filter_float() failing for ints
-Status: Open
+Status: Verified
-Package: FPM related
+Package: Filter related
-Assigned To:
+Assigned To: stas
```

**[2022-01-31 14:47 UTC] cmb@php.net**

```
Thanks for reporting; I can confirm this issue.  Suggested patch:

<https://gist.github.com/cmb69/b05cceb34e310438ab960ec3bbd1a59b>

Stas, can you please handle this?  Note that for PHP-8.1+ the
SKIPIF section should be replaced by:

--EXTENSIONS--
filter
```

**[2022-02-14 06:00 UTC] git@php.net**

```
Automatic comment on behalf of cmb69 (author) and smalyshev (committer)
Revision: https://github.com/php/php-src/commit/dce5e561a63fc970de722636ad8c09e9b079e8ae
Log: Fix #81708: UAF due to php_filter_float() failing for ints
```

### [2022-02-14 06:00 UTC] git@php.net

```
-Status: Verified
+Status: Closed
```

### [2022-02-14 06:00 UTC] git@php.net

```
Automatic comment on behalf of cmb69 (author) and smalyshev (committer)
Revision: https://github.com/php/php-src/commit/82f1bf1b6bc3a43aba62214870e6d0931e93a6d9
Log: Fix #81708: UAF due to php_filter_float() failing for ints
```

### [2022-02-14 06:07 UTC] stas@php.net

```
-CVE-ID:
+CVE-ID: 2021-21708
```

Last updated: Fri Dec 16 13:05:56 2022 UTC