Sec Bug #81739 OOB read due to insufficient input validation in imageloadfont()

Submitted: 2022-10-12 16:13 UTC
Modified: 2022-10-24 00:58 UTC
From: cmb@php.net
Assigned: stas (profile)
Status: Closed
Package: GD related
PHP Version: 7.4Git-2022-10-12 (Git)
OS: *
Private report: No
CVE-ID: 2022-31630

View | Add Comment | Developer | Edit

[2022-10-12 16:13 UTC] cmb@php.net

```
Description:
------------
It is possible to construct font files supposed to be loaded by
imageloadfont() which trigger OOB reads if the fonts are actually
accessed (e.g. by imagechar()).  The given test scripts exploits
that by triggering the assignment of a zero byte memory allocation
to gdFont.data (which is happily accepted by imageloadfont()), and
to read beyond this "buffer" when calling imagechar().

So if an application allows to upload arbitrary font files and
working with these, it is likely vulnerable.


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

$s = fopen(__DIR__ . "/font.font", "w");
// header without character data
fwrite($s, "\x01\x00\x00\x00\x20\x00\x00\x00\x08\x00\x00\x00\x08\x00\x00\x00");
fclose($s);
$font = imageloadfont(__DIR__ . "/font.font");
$im = imagecreate(10, 10);
imagechar($im, $font, 0, 0, " ", imagecolorallocate($im, 255, 255, 255));


Actual result:
--------------
OOB read (not unlikely resulting in a segfault, but could be worse).
```

Patches

Add a Patch

Pull Requests

Add a Pull Request

History

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

[2022-10-12 16:14 UTC] cmb@php.net

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

[2022-10-12 18:17 UTC] stas@php.net

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

[2022-10-18 10:17 UTC] cmb@php.net

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

[2022-10-18 10:17 UTC] cmb@php.net

This issue has been introduced with commit 88b6037[1], so versions
prior to PHP 7.4.0 are not affected. We could simply revert that
commit, but maybe it is better to duplicate the overflow check to
avoid confusion.

Suggested patch: <https://gist.github.com/cmb69/7155d511152bdf40a0b2c0105c65e905>.

When merging the test into PHP-8.1, please replace the --SKIPIF-- section with
--EXTENSIONS--
gd

[1] <https://github.com/php/php-src/commit/88b603768f8e5074ad5cbdccc1e0779089fac9d0>

[2022-10-24 00:44 UTC] stas@php.net

```
-CVE-ID: needed
+CVE-ID: 2022-31630
```

[2022-10-24 00:58 UTC] stas@php.net

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

[2022-10-24 00:58 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.