# Sec Bug #79329 get_headers() silently truncates after a null byte

**Submitted:** 2020-03-01 18:40 UTC **Modified:** 2020-03-17 05:39 UTC
**From:** 64796c6e69 at gmail dot com **Assigned:** stas (profile)
**Status:** Closed **Package:** *URL Functions
**PHP Version:** Irrelevant **OS:** any
**Private report:** No **CVE-ID:** 2020-7066

View | Add Comment | Developer | Edit

### [2020-03-01 18:40 UTC] 64796c6e69 at gmail dot com

```
Description:
------------
get_headers() silently truncates anything after a null byte in the URL it uses.

This was tested on PHP 7.3, but the function has always had this bug.

The test script shows that this can cause well-written scripts to get headers for an unexpected domain. Those headers
could leak sensitive information or unexpectedly contain attacker-controlled data.

Test script:
---------------
<?php
// user input
$_GET['url'] = "http://localhost\0.example.com";

$host = parse_url($_GET['url'], PHP_URL_HOST);
if (substr($host, -12) !== '.example.com') {
    die();
}
$headers = get_headers($_GET['url']);
var_dump($headers);

Expected result:
----------------
Warning: get_headers() expects parameter 1 to be a valid path, string given in php shell code on line 1
NULL

Actual result:
--------------
headers from http://localhost
```

## Patches

Add a Patch

## Pull Requests

Add a Pull Request

## History

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

### [2020-03-02 08:33 UTC] cmb@php.net

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

### [2020-03-02 08:33 UTC] cmb@php.net

```
Indeed, get_headers()'s $url has to be a valid path, because we're
passing it to php_stream_open_wrapper_ex().


 ext/standard/url.c | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/ext/standard/url.c b/ext/standard/url.c
index 57fd80cc1d..fe6d7f9de1 100644
--- a/ext/standard/url.c
+++ b/ext/standard/url.c
@@ -680,7 +680,7 @@ PHP_FUNCTION(get_headers)
        php_stream_context *context;

        ZEND_PARSE_PARAMETERS_START(1, 3)
-               Z_PARAM_STRING(url, url_len)
+               Z_PARAM_PATH(url, url_len)
                Z_PARAM_OPTIONAL
                Z_PARAM_LONG(format)
                Z_PARAM_RESOURCE_EX(zcontext, 1, 0)


I don't see the need for an regression test (ZPP only).
```

### [2020-03-02 18:32 UTC] stas@php.net

```
Note: the code in the test script is in no way secure. parse_url() does not guarantee the resulting URL is valid (or
even HTTP URL) - it just tries its best to parse it in assumption it's valid. If you need URL validation (as you
should if you importing external URLs) other methods should be used.

That said. no reason for get_headers() to accept URLs with nulls, so it shouldn't.
```

### [2020-03-02 18:48 UTC] 64796c6e69 at gmail dot com

@stas That's true. I may have oversimplified the example. My main point to get across was that even if validation exists, it wouldn't necessarily check the subdomain using a whitelist. There are too many characters valid in subdomains now:
https://stackoverflow.com/questions/7111881/what-are-the-allowed-characters-in-a-subdomain/22319900#22319900

**[2020-03-16 00:29 UTC] stas@php.net**

```
-CVE-ID:
+CVE-ID: 2020-7066
```

**[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=0d139c5b94a5f485a66901919e51faddb0371c43
Log: Fix bug #79329 - get_headers should not accept \0

**[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=69fdc14152edefd75a33be7fe87d1194098c67f7
Log: Fix bug #79329 - get_headers should not accept \0

**[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=335547a04d133e757c044dfa7cd78ab685939924
Log: Fix bug #79329 - get_headers should not accept \0

**[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=2bc92a0cf79e52e2096e45987468740d5bc748ed
Log: Fix bug #79329 - get_headers should not accept \0

**[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=f930ff52f45620eec2b2960f9e0a96d258ca1891
Log: Fix bug #79329 - get_headers should not accept \0

**[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=69fdc14152edefd75a33be7fe87d1194098c67f7
Log: Fix bug #79329 - get_headers should not accept \0

**[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=335547a04d133e757c044dfa7cd78ab685939924
Log: Fix bug #79329 - get_headers should not accept \0

**[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=0d139c5b94a5f485a66901919e51faddb0371c43
Log: Fix bug #79329 - get_headers should not accept \0

**[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=a33d05b1474caee449b88f53d61bee720c57caf7
Log: Fix bug #79329 - get_headers should not accept \0