New issue

Jump to bottom

emlog v6.0.0 zip plugin getshell vulnerability #1

Open **pwnninja** opened this issue on Dec 30, 2019 · 0 comments

pwnninja commented on Dec 30, 2019 • edited Owner

Vendor: emlog CMS https://www.emlog.net/
Tested Version: v6.0.0

Vulnerability in include/lib/function.base.php line 765:

```
function emUnZip($zipfile, $path, $type = 'tpl') {
if (!class_exists('ZipArchive', FALSE)) {
return 3;
}
$zip = new ZipArchive();
if (@$zip->open($zipfile) !== TRUE) {
return 2;
}
$r = explode('/', $zip->getNameIndex(0), 2);
$dir = isset($r[0]) ? $r[0] . '/' : '';
switch ($type) {
case 'tpl':
$re = $zip->getFromName($dir . 'header.php');
if (false === $re)
return -2;
break;
case 'plugin':
$plugin_name = substr($dir, 0, -1);
$re = $zip->getFromName($dir . $plugin_name . '.php');
//We can upload a zipfile and extract a php webshell later
if (false === $re)
return -1;
break;
case 'backup':
$sql_name = substr($dir, 0, -1);
if (getFileSuffix($sql_name) != 'sql')
return -3;
break;
case 'update':
break;
}
if (true === @$zip->extractTo($path)) {
$zip->close();
return 0;
} else {
return 1;
}
}
```

POC:
http://x.x.x.x/emlog/src/admin/plugin.php
We upload abc.zip which contains abc/abc.php
Then we access http://x.x.x.x/emlog/src/content/plugins/abc/abc.php

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant