alexmackey fix merge

History

1 contributor

76 lines (57 sloc) | 3.8 KB

Issue CVE-2022-40407

Chamilo LMS Authenticated RCE via malicious zip file upload (ZipSlip)

- Versions: Chamilo v1.11, Chamilo v1.10 and earlier
- CVE: CVE-2022-40407
- Chamilo Issue Description and Fix

Summary

Chamilo versions prior to v1.11.16 are vunerable to ZipSlip vunerability that can be exploited by crafting malicious zip file to gain RCE (Remote Code Execution).

This issue can be exploited as both standard and administrative users although steps differ.

Reported to Chamilo 6th Sep 2022 via Chamilo security issue reporting procedures.

Steps to reproduce

There are two main steps for this exploit:

- Create a malicious zip file
- Upload and trigger the extraction of the zip file as either user or admin

Create a malicious zip file

First create a malicious zip file that will navigate two directories up using path transversal and place a PHP file with content you specify at this location.

The below Python3 script will create a zip file called badzip.zip that calls `phpinfo()` when accessed:

```
#!/usr/bin/python
import zipfile
z_info = zipfile.ZipInfo("../../info.php")
z_file = zipfile.ZipFile("badzip.zip", mode="w")
z_file.writestr(z_info, "<?php phpinfo();?>")
z_file.close()
```

The next steps differ depending on whether this is being done as a standard user or administrator (less steps).

Admin RCE

1. Create a malicious zip file as above
2. Log-in as an administrative user
3. Create a new course or use an existing one
4. Go into the course
5. Go to documents
6. Select upload documents
7. Select Advanced Settings and ensure un-compress zip is selected (leave override file option on but dont think it matters)
8. Select the malicious zip file you created earlier
9. Click Upload File
10. The file will get uploaded and then extracted via the path to `/app` and can be accessed at `http://localhost/chamilo-1.11/app/info.php`

User RCE

You will need a user login and to be assigned to at least one course with an assignment.

1. Create a malicious zip file as above
2. Log in as student user
3. Go to assignments
4. Select an assignment
5. Select Upload (Simple)
6. Give the item a title and select your malicious zip file
7. Next fire up a Proxy (e.g. Burp Community) as you'll need it to modify one of the requests before it is sent. Ensure you have the browser set to use the proxy if you have not already
8. Click upload
9. The proxy will capture the requests.
10. Chamilo issues 3 requests to upload a file.
11. Let the first 2 continue to Chamilo un-modified
12. On the 3rd and final request (the one that ends `action=finish` e.g. `/chamilo-1.11/main/inc/lib/javascript/bigupload/inc/bigUpload.php?action=finish`) we need to modify it so we can trick Chamilo into extracting the uploaded file even through extract functionality is not available in the UI for the student. To do this do the following:

- Change the origin parameter in the body to `document`
- Add the following parameters: `unzip=1`, `if_exists=overwrite` and `curdirpath = "/"`
- Your final request body should look something like the following

```
key=3242343.tmp&name=badzip.zip&type=application/zip&size=182&origin=document&title=test&extension=&_qf__form-work=&contains_file=0&active=1&unzip=1&if_exists=overwrite&curdirpath=/&accepted=1&MAX_FILE_SIZE=2097152&id=1&sec_token=324234
```

13. Send the modified request
14. The file will get uploaded and then extracted via the path to `/app` and can be accessed at `/chamilo-1.11/app/info.php`

Alex Mackey 6th Sep 2022