Authenticated Arbitrary File Write via BigUpload endpoint (<=1.11.36)

High **ywarnier** published **GHSA-phfx-pwwg-945v** 5 hours ago

Package

php **chamilo/chamilo-lms** (Composer)

Affected versions	Patched versions
<=1.11.36	1.11.38

Description

Summary

Any authenticated user (including students) can write arbitrary content to files on the server via the BigUpload endpoint. The `key` parameter controls the filename and the raw POST body becomes the file content. While `.php` extensions are filtered to `.phps`, the `.pht` extension passes through unmodified. On Apache configurations where `.pht` is handled as PHP, this leads to Remote Code Execution.

Details

Affected code: `main/inc/lib/javascript/bigupload/inc/bigUpload.php`

The `uploadFile()` method reads raw POST data from `php://input` and writes it to `$tempDirectory . $tempName` without sufficient filename validation:

```
public function uploadFile()
{
    $fileData = file_get_contents('php://input');
    $handle = fopen($this->getTempDirectory().$this->getTempName(), 'a');
    fwrite($handle, $fileData);
    fclose($handle);
}
```

The `setTempName()` method calls `disable_dangerous_file()` which converts `.php` to `.phps`, but `.pht` is not in the blocklist.

Files are written to `/var/www/chamilo/app/cache/` which is web-accessible.

Impact

- Authenticated users (including students) can write arbitrary content to server filesystem
- `.pht` extension bypasses the filename filter
- On Apache with `AddHandler application/x-httpd-php .pht` (common in many distributions), this results in Remote Code Execution
- Even without PHP execution, arbitrary file write can be used for denial of service (disk filling) or planting malicious content
- Path traversal is blocked (`../` is stripped), limiting writes to `/app/cache/`

Severity

High 7.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L

CVE ID

CVE-2026-33704

Weaknesses

▶ CWE-434