6 Arbitrary File Deletion via Path Traversal in image-edit.php

Share:

TIMELINE

egix submitted a report to ImpressCMS. Jan 19th (2 years ago)

Summary:

The vulnerability is located in the `/libraries/image-editor/image-edit.php` script:

Code 437 Bytes — Wrap lines Copy Download

```
1  161.     if (@copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp, $categ_path . $simage->getVar ( 'image_name' ) )) {
2  162.         if (@unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp )) {
3  163.             $msg = _MD_AM_DBUPDATED;
4
5  [...]
6
7  190.     } else {
8  191.         if (copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp, $categ_path . $imgname )) {
9  192.             @unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp );
10 193.             }
```

User input passed through the "image_temp" parameter is not properly sanitized before being used in a call to the `unlink()` function at lines 162 and 192. This can be exploited to carry out Path Traversal attacks and delete arbitrary files in the context of the web server process.

NOTE: before being deleted, the file will be copied into the `/uploads/imagemanager/logos/` directory. As such, by firstly deleting the `index.html` file in that directory, it might be possible to disclose the content of arbitrary files in case the web server allows for directory listing.

ImpressCMS branch :

The vulnerability has been tested and confirmed on ImpressCMS version 1.4.2 (the latest at the time of writing).

Steps To Reproduce:

1. Login into the application as any user (this should work both for Webmasters and Registered Users)
2. Go to: `http://[impresscms]/libraries/image-editor/image-edit.php?op=save&image_id=1&image_temp=../../../mainfile.php`
3. The `mainfile.php` script will be deleted, rendering the website unusable

Impact

This vulnerability might allow authenticated attackers to delete arbitrary files, potentially leading to a Denial of Service (DoS) condition or destruction of users data.

fiammybe ImpressCMS staff changed the status to o **Triaged**. Jan 29th (2 years ago)

Thank you for this! In other areas, I have stopped this by rewriting double points (..) to underscores. That would disallow path traversal. I'll include this ASAP. I believe it is both in 1.4.x and 2.0 (pre-release)?

egix posted a comment. Jan 29th (2 years ago)

Hi @fiammybe! Yes, it looks like this affects version 2.0.0 Alpha 10 as well.

egix posted a comment. Feb 3rd (2 years ago)

Hi @fiammybe,

the Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2021-26601 to this vulnerability.

fiammybe ImpressCMS staff posted a comment. Feb 3rd (2 years ago)

Hi @egix , thanks! I didn't know there was the possibility of a CVE number (nobody requested one for us until now). I learned, thank you very much.

fiammybe ImpressCMS staff posted a comment. Feb 11th (10 months ago)

This has been resolved in 1.4.3

egix posted a comment. Feb 11th (10 months ago)

@fiammybe I confirm this has been resolved in 1.4.3. Please feel free to close this report.

fiammybe ImpressCMS staff closed the report and changed the status to o **Resolved**. Feb 20th (10 months ago)

resolved in ImpressCMS 1.4.3

egix requested to disclose this report. Feb 20th (10 months ago)

This report has been disclosed. Mar 22nd (9 months ago)