Home / Advisories / Zenario CMS 9.2 Insecure file upload (RCE)

Zenario CMS 9.2 - Insecure file upload (RCE)

Summary

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Affected versions	9.2
Fixed versions	9.2.55826
State	Public
Release date	2022-02-18

Vulnerability

Kind	Insecure file upload (RCE)
Rule	027. Insecure file upload
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVSSv3 Base Score	9.1
Exploit available	No
CVE ID(s)	CVE-2022-23043

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Proof of Concept

Steps to reproduce

1. Once login as admin click on 'Go to Organizer'> 'Configuration'.
2. Select 'File/MIME Types' in the 'Configuration' menu.
3. Click on 'Create'.
4. Create a new custom file type using 'phar' as extension and 'text/plain' as MIME Type and then click on 'Save'.

The server validates some malicious extensions but still there are some valid executable extensions. For example 'phar' and 'shtml'.

5. Create a '.phar' file with the following content.

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

6. On the admin menu, click on 'Documents'
7. Click on 'Upload documents'
8. Click on 'Upload...' and browse the created file.
9. Select 'Public' and click on 'Save'.
10. Select the file and click on 'Actions' > 'View public link' in order to get the file

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

- Operating System: Linux.
- Web Server: Apache
- PHP Version: 7.4
- Database and version: Mysql

Exploit

There is no exploit for the vulnerability but can be manually exploited.

Mitigation

An updated version of Zenario CMS is available at the vendor page.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks`.

References

Vendor page https://zenar.io/

Patched version
https://github.com/TribalSystems/Zenario/releases/tag/9.2.55826

Timeline

- ✓ 2022-01-13
  Vulnerability discovered.

- ✓ 2022-01-13
  Vendor contacted

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

- ✓ Public Disclosure.

Services

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details