Home / Advisories / Exponent CMS 2.6.0 patch2 Insecure file upload (RCE)

Exponent CMS 2.6.0 patch2 - 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	v2.6.0 patch2
State	Public
Release Date	2022-02-03

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-2022-23048

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

1. Click on the Exponent logo located on the upper left corner.
2. Go to 'Super-Admin Tools' > 'Extensions' > 'Install Extension'.
3. Click on 'Upload Extension'.
4. Create a malicious PHP file with the following PoC.

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

5. Zip the php file.

6. Upload the zip file.

7. Click on 'Upload Extension'

8. Next, click on 'Continue with Installation'.

9. Go to `http://127.0.0.1/exponentcms/themes/simpletheme/{rce}.php` in order to execute commands.

System Information:

- Version: Exponent CMS 2.6.0 patch2.
- Operating System: Linux.
- Web Server: Apache
- PHP Version: 7.4

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

Mitigation

By 2022-02-03 there is not a patch resolving the issue.

Credits

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

References

Vendor page https://www.exponentcms.org/

Ticket https://exponentcms.lighthouseapp.com/projects/61783/tickets/1460

Issue https://github.com/exponentcms/exponent-cms/issues/1546

Timeline

- 2022-01-24
  Vulnerability discovered.
- 2022-01-24
  Vendor contacted.
- 2022-02-03
  Public Disclosure.

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

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

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

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

Service Status - Terms of Use - Privacy Policy - Cookie Policy