



attacks

[Home](#) / [Advisories](#) / [Exponent CMS 2.6.0 patch2 Stored XSS \(User-Agent\)](#)

Exponent CMS 2.6.0 patch2 – Stored XSS (User-Agent)

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	Stored cross-site scripting (XSS)
Rule	<u>010. Stored cross-site scripting (XSS)</u>
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CVSSv3 Base Score	5.4
Exploit available	No
CVE ID(s)	<u>CVE-2022-23049</u>



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. Use a Web proxy or a tool to modify the browser User-agent with the following PoC.

```
User-Agent: <script>alert('XSS')</script>
```

2. Try to login with a non-admin user.
3. If an admin user visits 'User Management' > 'User Sessions' the XSS will be triggered.

A non-admin user may compromise an admin session by exploiting this vulnerability.

System Information:

- Version: Exponent CMS 2.6.0 patch2.
- 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



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

FLUID ATTACKS .

References

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

Ticket <https://exponentcms.lighthouseapp.com/projects/61783/tickets/1461>

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

Timeline

- 2022-01-25
✓ Vulnerability discovered.

- ✓ 2022-01-25
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](#)

[FAQ](#)

[Documentation](#)

[Contact](#)



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](#)