Exponent CMS 2.6.0 patch2 - Stored XSS

Summary

Affected versions	v2.6.0 patch2
State	Public
Release Date	2022-02-03

Vulnerability

Kind	Stored cross-site scripting (XSS)
Rule	010. Stored cross-site scripting (XSS)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
CVSSv3 Base Score	4.8
Exploit available	No
CVE ID(s)	CVE-2022-23047

Proof of Concept

1. Click on the Exponent logo located on the upper left corner.
2. Go to 'Configure Website'.
3. Update the 'Site Title' field or any of the vulnerable fields with the following PoC.

```
Exponent CMS" onmouseover=alert('xss')>
```

4. If a user hover the mouse over the logo or visits the 'Configure Website' the XSS will be triggered.

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

References

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

Ticket https://exponentcms.lighthouseapp.com/projects/61783/tickets/1459

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.

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing