Exponent CMS 2.6.0 patch2 Stored Cross-Site Scripting Vulnerability #1459 new

Reported by Oscar | January 24th, 2022 @ 04:38 PM

(#bug-description) Bug description

Exponent CMS **2.6.0 patch2** allows an authenticated admin user to inject persistent javascript code inside the "Site/Organization Name,Site Title and Site Header" parameters while updating the site settings on http://127.0.0.1/exponentcms/administration/configure_site (http://127.0.0.1/exponentcms/administration/configure_site) .

(#cvssv3-vector-cvss-3-1-av-n-ac-l-pr-h-ui-r-s-c-c-l-i-l-a-n) 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) CVSSv3 Base Score: 4.8
(#steps-to-reproduce) Steps to reproduce

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 "Site/Organization Name","Site Title" or "Site Header") 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.

Attached below are the links to the advisory and our responsible disclosure policy.

- https://fluidattacks.com/advisories/franklin/ (https://fluidattacks.com/advisories/franklin/)
- https://fluidattacks.com/advisories/policy (https://fluidattacks.com/advisories/policy)

(#system-information) System Information

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

- Xss_huge xss.png 99.1 KB delete

Comments and changes to this ticket

dleffler

February 12th, 2022 @ 09:43 PM

Assigned user changed from “expNinja” to “dleffler”

I think our approach has been that Admin users must be trusted. There's a lot of malicious stuff an Admin user can do.

Restore?

(This comment has been marked as spam)