New issue

Jump to bottom

Exponent-CMS Security Issues #1546

Open **alestorm980** opened this issue on Jan 28 · 2 comments

Labels security

alestorm980 commented on Jan 28 • edited

I reported 3 vulnerabilities on Exponent 2.6.0 (patch2) using https://exponentcms.lighthouseapp.com/ but i didn't receive any update.

Attached below are the links to the tickets, advisories and our responsible disclosure policy respectively.

- Ticket Stored XSS (Settings).
- Advisory Stored XSS (Settings).
- Ticket File Upload RCE (New Extension)
- Advisory File Upload RCE (New Extension).
- Ticket Stored XSS (User-Agent)
- Advisory Stored XSS (User-Agent).
- Disclosure Policy.

dleffler commented on Feb 12 Collaborator

As stated on our obsolete bug reporting site (Lighthouse), the XSS Settings and RCE issues only apply to Super-Admin or Admin users and users with that level of permission can do quite a bit to hack a site...However, the User-Agent issue should be addressed.

 **dleffler** added the security label on Feb 12

dleffler commented on Feb 12 Collaborator

Fix for the XSS User Agent issue has be added to development code and will be included in next release

Assignees

No one assigned

Labels

security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants