Exponent CMS 2.6.0 patch2 Stored Cross-Site Scripting (User-Agent) #1461 ✓resolved

Reported by Oscar | January 25th, 2022 @ 03:42 PM

(#bug-description) Bug description

Exponent CMS **2.6.0 patch2** allows an authenticated user to inject Javascript code on the User-Agent when logging in.
When an administrator user visits the 'User Sessions' tab, the Javascript will be triggered allowing an attacker to compromise the administrator session.

(#cvssv3-vector-cvss-3-1-av-n-ac-l-pr-l-ui-r-s-c-c-l-i-l-a-n) 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) CVSSv3 Base Score: 5.4
(#steps-to-reproduce) Steps to reproduce

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' page, the XSS will be triggered.

(#impact) Impact

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

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

https://fluidattacks.com/advisories/cobain/
(https://fluidattacks.com/advisories/cobain/)
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

Comments and changes to this ticket

Oscar

January 25th, 2022 @ 05:28 PM

no changes were found...

xss.gif 1.2 MB

dleffler

February 12th, 2022 @ 09:44 PM

Assigned user changed from “expNinja” to “dleffler”

I will work on a fix, but the v2.6.0patch3 release was issued already today.

dleffler

February 13th, 2022 @ 01:28 AM

State changed from “new” to “resolved”

Fix uploaded to development code. Will be included in next release