Exponent CMS 2.6.0 patch2 - Insecure file upload (RCE Upload new extension) #1460 new

Reported by Oscar | January 24th, 2022 @ 05:32 PM

(#bug-description) Bug description

Exponent CMS **2.6.0 patch2** allows an authenticated admin user to upload a malicious extension in the format of a zip file with a php file inside it.
After uploaded it, the php file will be placed at `themes/simpletheme/{rce}.php` from where can be accessed to execute commands.

(#cvssv3-vector-cvss-3-1-av-n-ac-l-pr-h-ui-n-s-c-c-h-i-h-a-h) CVSSv3 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
(#cvssv3-base-score-9-1) CVSSv3 Base Score: 9.1
(#steps-to-reproduce) Steps to reproduce

1. Click on the Exponent logo located on the upper left corner.
2. Go to 'Super-Admin Tools' > 'Extensions' > 'Install Extension'.
3. Click on 'Upload Extension'.
4. Create a malicious PHP file with the following PoC.

```
<?php echo system($_GET['cmd']); ?>
```

1. Zip the php file.
2. Upload the zip file.
3. Click on 'Upload Extension'
4. Next, click on 'Continue with Installation'.
5. Go to `http://127.0.0.1/exponentcms/themes/simpletheme/{rce}.php` in order to execute commands

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

- https://fluidattacks.com/advisories/dylan/ (https://fluidattacks.com/advisories/dylan/)
- 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

- Rce_huge rce.gif 2.2 MB

Comments and changes to this ticket

dleffler

February 12th, 2022 @ 09:40 PM

Assigned user changed from “expNinja” to “dleffler”

I'm not sure I follow your logic. A Super-Admin by definition is granted permission to pretty well take down the site any number of ways?

Oscar

February 17th, 2022 @ 04:12 PM

Any functionality that allows functions/actions other than those planned are cases of abuse, regardless of the context (the impact is given by the rating). Abuse cases are usually vulnerabilities that need to be fixed.