Unrestricted Upload of File with Dangerous Type in jsdecena/laracom

0

Valid Reported on Jan 21st 2022

Description

Hi there, I would like to report a vulnerability that allows a hacker to upload dangerous file type in jsdecena/laracom.
Attacker must have an account with permission to Edit Product (E.g. `Clerk` role).
Then, he can upload malcious file with extensions such as html, svg,... which leads to XSS.

Proof of Concept

After login, go to `Products / List Products`, click on `Actions / Edit`.
In `Cover` or `Images` fields, upload html files with xss payload inside. For example: `<script> alert(document.cookie) </script>`.
Click on `update` button to save.
Demo Video: https://drive.google.com/file/d/1BsfbHp1I47E02ZKaa6ZhcjmHMxD6Jho4/view?usp=sharing

Impact

This vulnerability is capable of uploading dangerous file to serve

CVE
CVE-2022-0472
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (8.1)

Visibility
Public

Status
Fixed

Found by

supernaruto16
@supernaruto16
unranked

This report was seen 337 times.

We are processing your report and will contact the **jsdecena/laracom** team within 24 hours.
10 months ago

We have contacted a member of the **jsdecena/laracom** team and are waiting to hear back
10 months ago

We have sent a follow up to the **jsdecena/laracom** team. We will try again in 7 days.
10 months ago

We have sent a second follow up to the **jsdecena/laracom** team. We will try again in 10 days.
10 months ago

A **jsdecena/laracom** maintainer validated this vulnerability 10 months ago

supernaruto16 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **jsdecena/laracom** maintainer marked this as fixed in **v2.0.9** with commit **256026**
10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation