Unrestructed file upload in yetiforcecompany/yetiforcecrm

0

Valid Reported on Apr 14th 2022

Description

I found unrestricted file upload leads to xss, vulnerability can be exploited by uploading a crafted payload inside a file. Then, the vulnerability can be triggered when the user previews the files content.

Proof of Concept

```
unrestricted file upload payload
https://drive.google.com/file/d/1DQs5LKkndhwNhKmEaSUIgs6z7HlJybap/view?usp=

Injection point
https://drive.google.com/file/d/1xLgMCTzVhQuWY7wnFEdx3FWLRsUShrtQ/view?usp=

POC
https://drive.google.com/file/d/1oX3BnHhE5c6hwbPxYPvCpr8P34UK79Cu/view?usp=
```

Impact

Attacker can send malicious files to the victims is able to retrieve the stored data from the web application without that data being made safe to render in the browser and steals victim's cookie leads to account takeover.

Occurrences

Accounts.php L26-L135

References

- https://hackerone.com/reports/765679

CVE
CVE-2022-1411
(Published)

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

Severity
Critical (9.1)

Registry
Other

Affected Version
latest

Visibility
Public

Status
Fixed

Found by

Raptor
@aravindd007
amateur

Fixed by

Mariusz Krzaczkowski
@mariuszkrzaczkowski
maintainer

This report was seen 577 times.

We are processing your report and will contact the yetiforcecompany/yetiforcecrm team within 24 hours. 7 months ago

We have contacted a member of the yetiforcecompany/yetiforcecrm team and are waiting to

hear back 7 months ago

Mariusz 7 months ago Maintainer

give more details on how to induce a vulnerability because we can't find it

Raptor 7 months ago Researcher

Sir, Upload the given payload drive link, and inspite element open the upload link path , you got pop-up.

Raptor 7 months ago Researcher

Sir, If you didn't understand please reply me.

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

Radosław 7 months ago Maintainer

Sorry for the delayed reply, we had some days off due to holidays.
Back to the topic...
I understand, the problem is that the image is temporarily displayed by one of CKEditor's plugins.

Radosław Skrzypczak validated this vulnerability 7 months ago

Raptor has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 7 days. 7 months ago

We have sent a second fix follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 10 days. 7 months ago

Mariusz Krzaczkowski marked this as fixed in **6.4.0** with commit **bf69c4** 7 months ago

Mariusz Krzaczkowski has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Accounts.php#L26-L135 has been validated ✔

Sign in to join this conversation