huntr

# Cross-site Scripting (XSS) - Stored in yetiforcecompany/yetiforcecrm

0

✓ Valid Reported on Apr 11th 2022

## Description

Stored Cross-Site Scripting (XSS) vulnerability due to the lack of content validation and output encoding. This vulnerability can be exploited by uploading a crafted payload inside a document. Then, the vulnerability can be triggered when the user previews the document´s content.

## Proof of Concept

```
https://drive.google.com/file/d/1xJh3wjyBUB5JF0rsbPblrUUREvtHA-EG/view?usp=
```

## Impact

Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then a victim is able to retrieve the stored data from the web application without that data being made safe to render in the browser.

## Occurrences

Accounts.php L59-L298

## References

- https://owasp.org/www-community/Types_of_Cross-Site_Scripting

CVE
CVE-2022-1340
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7)

Registry
Other

Affected Version
latest

Visibility
Public

Status
Fixed

Found by

Raptor
@aravindd007
amateur

This report was seen 659 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

Radosław 7 months ago Maintainer

Hey @aravindd007,
thanks for the report.
I have two comments and one request, however.

I think the error category is wrong, because you can't save xss permanently, t
example.
DOM-Based XSS seems more accurate.

Chat with us

Correct me if I'm wrong.

The file you mentioned has nothing to do with the reported vulnerability.

Could you verify whether this vulnerability also exists in the dev environment (https://gitdeveloper.yetiforce.com/)?

Raptor 7 months ago Researcher

The input not sanitized properties, yes I can't save permanently is possible to bypass, we can do html injection, iframe injection also.

Yes that is dev environment.

Radosław 7 months ago Maintainer

Apologies in advance for continuing this discussion but I'm not sure I understood you.
In my opinion there is no way of saving xss permanently in the system regardless of what means of bypassing it were used, since all data are verified additionally on the server side before they're entered to the database for example.

Nevertheless, a few fixes have been uploaded to the dev environment. I'd appreciate if you could check if everything is ok now.

Radosław Skrzypczak validated this vulnerability 7 months ago

Raptor has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

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

We have sent a third and final fix follow up to the **yetiforcecompany/yetiforcecrm** team. This report is now considered stale. 7 months ago

Radosław Skrzypczak marked this as fixed in **6.4.0** with commit **2c14ba** 3

The fix bounty has been dropped ✗

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Accounts.php#L59-L298 has been validated ✓

thanhlocpanda 3 months ago

@Maintainer You should reject this vulnerability, It couldn't store the user input and it does not have any impact.  The PoC does not show anything. Assign this CVE will make your CRM's reputation is decrease.

Raptor 3 months ago Researcher

@thanhlocpanda copy my report.

Sign in to join this conversation

privacy policy

Chat with us