

# Persistent Cross Site Scripting - LayoutEditor Module - Settings in yetiforcecompany/yetiforcecrm

0



Valid

Reported on Aug 19th 2022

## Description

The application uses Purifier to avoid the Cross Site Scripting attack. However, On LayoutEditor module from Settings, the type of fieldModel->label parameter is "Text" but it is not validated and it's used directly without any encoding or validation on LayoutEditor/EditField.tpl. It allows attacker to inject arbitrary Javascript code to perform an Stored XSS attack.

## Proof of Concept

- 1- Login to the application
- 2- Access the LayoutEditor Module via the following URL:  
<https://gitstable.yetiforce.com/index.php?module=LayoutEditor&parent=Settings&view=Index>
- 3- Click to the button "Edit", Change the value of "label" parameter with the following payload:

```
LayoutEditor" onfocus="alert(document.domain)" autofocus ""=
```

**\*\*Inject the payload**

Chat with us



An XSS attack allows an attacker to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.

## Occurrences

 EditField.tpl L41

CVE

CVE-2022-3000  
(Published)

Vulnerability Type

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

Severity

Medium (6.3)

Registry

Other

Affected Version

6.4.0

Visibility

Public

Status

Fixed

Found by



thanhlocpanda

@thanhlocstudent

master 

This report was seen 736 times.

We are processing your report and will contact the **yetiforcecompany/yetiforcecrm** team within 24 hours. 3 months ago

thanhlocpanda modified the report 3 months ago

Chat with us

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

we have contacted a member of the **yetiforcecompany/yetiforcecrm** team and are waiting to hear back. 3 months ago

**thanhlocpanda** modified the report. 3 months ago

**thanhlocpanda** modified the report. 3 months ago

We have sent a follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 7 days. 3 months ago

**thanhlocpanda** modified the report. 3 months ago

**Radosław Skrzypczak** validated this vulnerability. 3 months ago

**thanhlocpanda** 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. 3 months ago

We have sent a second fix follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 10 days. 3 months ago

We have sent a third and final fix follow up to the **yetiforcecompany/yetiforcecrm** team. This report is now considered stale. 2 months ago

**thanhlocpanda** 2 months ago

Researcher

Hi @admin, the bug has been fixed by @rskrzypczak, please help me review and publish the CVE. You can check with the following commit:  
<https://github.com/YetiForceCompany/YetiForceCRM/commit/eebc12601495ada38495076bec12841b2477516b#diff-09030a439bec9e66dd7a588b2558d8b88ab84cf9ecf03c5de96a042f1be1b332>

**Radosław Skrzypczak** marked this as fixed in 6.4.0 with commit **eebc12**. 2 months ago

The fix bounty has been dropped. ✗

This vulnerability will not receive a CVE. ✗

**EditField.tpl#L41** has been validated. ✓

Chat with us



Sign in to join this conversation

2022 © 418sec

## huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

## part of 418sec

[company](#)

[about](#)

[team](#)

Chat with us