Cross-Site Request Forgery (CSRF) in yetiforcecompany/yetiforcecrm

0

Valid Reported on Jan 12th 2022

Description

Hi there, I would like to report a CSRF vulnerability in yetiforcecompany/yetiforcecrm. This allows an attacker to create a new admin. Even when `SameSite: Strict` enable, this still can be exploited by an attacker with lowest privilege account (E.g. `guest`).

Proof of Concept

These are POCs for 2 scenario, both leads to create a new admin with username `testggwp` and password `Admin@123` .
Scenario 1: `SameSite` is `None` or `Lax`
Trick admin to access below link

```
/index.php?module=Users&parent=Settings&view=Edit&fromView=Create&action=Sa
```

Scenario 2: `Samesite` is `Strict`
Create a record in Documents with below payload in description (click source then paste). After that, trick Admin to visit the record.

```
<img src="/index.php?module=Users&parent=Settings&view=Edit&fromView=Create
```

Impact

After csrf payload is triggered, attacker can become an admin with full privil

References

References

- video poc for scenario 2 (samesite: strict)

CVE
CVE-2022-0269
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

supernaruto16
@supernaruto16
unranked

Fixed by

OUR YETI

Radosław Skrzypczak
@rskrzypczak
maintainer

This report was seen 404 times.

We are processing your report and will contact the **yetiforcecompany/yetiforcecrm** team within 24 hours. 10 months ago

We have contacted a member of the **yetiforcecompany/yetiforcecrm** team and are waiting to hear back 10 months ago

We have sent a follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 7 days. 10 months ago

Radosław 10 months ago Maintainer

Thank you for the report, We're currently working on a fix that will be released soon and then we'll take care of this report. Thanks.

Radosław Skrzypczak validated this vulnerability 10 months ago

supernaruto16 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Radosław Skrzypczak marked this as fixed in **6.3.0** with commit **298c78** 10 months ago

Radosław Skrzypczak has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation