Stored XSS in 'Table name' field via Database information function in yetiforcecompany/yetiforcecrm

0

Valid Reported on Aug 16th 2022

Description

When the administrator uses the Database information function, malicious code will be accidentally called and executed through two cases:
(1) An internal attacker (local) with access right to the database could insert malicious content into the `table name` field by creating a table in the database.
(2) The second possible case is when the system administrator performs a malicious import of the database from an unknown source with the `table name` field injected by malicious content.

Proof of Concept

Payload

```
CREATE TABLE `yetiforce`.`<script>alert('stored_xss')</script>` ( `id` INT
```

Reprodution steps

Step 1: The internal attacker create a new table with the payload above.
PoC - Step 1
Step 2: Access `Database information` function in Admin Dashboard > Logs > Server configuration
PoC - Step 2
Step 3: The XSS should fire immediately when detailed information about the database is loaded.
PoC - Step 3.1
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,...

References

- https://owasp.org/www-community/attacks/xss/

CVE
CVE-2022-2885
(Published)

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

Severity
Medium (6.7)

Registry
Other

Affected Version
6.3.0

Visibility
Public

Status
Fixed

Found by

0xb4c
@0xb4c
unranked

This report was seen 620 times.

We are processing your report and will contact the yetiforcecompany/yetifor... 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

Mariusz Krzaczkowski 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

Mariusz Krzaczkowski marked this as fixed in 6.4.0 with commit a9ad9e 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation