

SQL Injection in salesagility/suitecrm

0

✓ Valid

Reported on Feb 12th 2022

Description

In SuiteCRM v7.12.4, a malicious user can inject SQL query in order to affect the execution of predefined SQL commands impacting database leakage.

Proof of Concept

The `$_POST['record']` [1] parameter is controllable by a user and it is concatenated into SQL query [2] without validating them.

Source file:

<https://github.com/salesagility/SuiteCRM/blob/master/modules/ProspectLists/Duplicate.php#L62>

```
$focus->retrieve($_POST['record']); //[1]
if (isset($_POST['isDuplicate']) && $_POST['isDuplicate'] == true) {
    $focus->id='';
    $focus->name=$mod_strings['LBL_COPY_PREFIX'].' '.$focus->name;


    $focus->save();
    $return_id=$focus->id;
    //duplicate the linked items.
    $query = "select * from prospect_lists_prospects where prospect_list_i
    $result = $focus->db->query($query);
```

Impact

This vulnerability is capable of reading sensitive database related information such as read admin password hash and existing database data.

Chat with us

Occurrences

 Duplicate.php L62

CVE
CVE-2022-0754
(Published)

Vulnerability Type
CWE-89: SQL Injection



Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by



Faisal Fs 
@faisalFs10x
unranked 

Fixed by



Matt Lorimer
@mattlorimer
maintainer

This report was seen 756 times.

We are processing your report and will contact the **salesagility/suitecrm** team within 24 hours.
9 months ago

Faisal Fs  modified the report 9 months ago

We have contacted a member of the **salesagility/suitecrm** team and are waiting for a response.
9 months ago

Chat with us

Hi Faisal,

Thank you for your Security Report(s).

We have raised this issue with our internal security team to be confirmed.

Below is a reference of the issue raised and ID allocated.

SCRMBT-#188 - SQL Injection in Prospects List

We will review the issue and confirm if it is a vulnerability within SuiteCRM and meets our criteria for a Security issue. If an issue is not considered a Security issue or that it does not need to be private then we'll raise it via the GitHub bug tracker or a more appropriate place.

Thank you for your contribution to the SuiteCRM project.

We have sent a follow up to the **salesagility/suitecrm** team. We will try again in 7 days.
9 months ago

A **salesagility/suitecrm** maintainer validated this vulnerability 9 months ago

Faisal Fs  has been awarded the disclosure bounty 

The fix bounty is now up for grabs

Hi Faisal,

The Security Team have now assessed the following issue:

SCRMBT-#188 - SQL Injection in Prospects List

This issue has been given a severity grading of 'Important'. Due to the severity of this issue we are working to release a fix for it very soon.

Once the fix is released, we aim to include your name in the release notes - giving credit for finding and reporting this issue. Please let us know if you would prefer not be referenced or have a specific request on how you would like to be referenced within the release notes.

Chat with us

Thank you for your assistance and contribution to the SuiteCRM product!

Researcher

Faisal Fs  9 months ago

You can use the name in the release notes as

Faisal Fs with @faisalfs10x as handle,
and company name NetbyteSEC, www.netbytesec.com.

Best wishes..

We have sent a fix follow up to the **salesagility/suitecrm** team. We will try again in 7 days.
9 months ago

We have sent a second fix follow up to the **salesagility/suitecrm** team. We will try again in 10 days.
9 months ago

Matt Lorimer marked this as fixed in **7.12.5** with commit **e93b26** 9 months ago

Matt Lorimer has been awarded the fix bounty 

This vulnerability will not receive a CVE 

Duplicate.php#L62 has been validated 

Sign in to join this conversation

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[about](#)

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)