Improper Access Control in salesagility/suitecrm

0

Valid Reported on Feb 13th 2022

Description

In SuiteCRM v7.12.4, affecting Users Module, any user with the User Type as Regular User could modify other users profiles via the update profile section. The prerequisite of this attack is by knowing the user record (ID) and username (User Name) respectively. The user records (ID) can be obtained in the employee section while the username (User Name) could be obtained via exporting employee records bug. The impact could lead to account take over due to the ability to modify related data in the update profile section including email and mobile numbers.

Proof of Concept

Affected endpoint:
1 POST http://{HOST}/index.php, parameter `record` & `user_name`
2 POST http://{HOST}/index.php
~
Steps to reproduce:
1 Login as a user with regular user role.
2 Go to profile section > Intercept request with burp suite > Click save button
3 Change `record` parameter to victim record such as `1` for the default admin
4 Change `user_name` parameter to `admin` for default admin.
5 Modify other information such as email or phone number if any and click forward request in burp.
6 Observe the changes in the admin profile.
~
Request file: Modify other user profile via the update profile section., pwd: `7Ty6DfTmuc4`
Request file: Downgrade Role from Admin to Regular user , pwd: `7Ty6DfTmuc4`

Impact

This vulnerability is capable of modifying someone else's account, by providi
identifier.

CVE
CVE-2022-0755
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

Matt Lorimer
@mattlorimer
maintainer

This report was seen 453 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

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Chat with us

Faisal Fs ⚔️ modified the report 9 months ago

We have contacted a member of the **salesagility/suitecrm** team and are waiting to hear back

9 months ago

Jack Anderson 9 months ago Maintainer

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-#189 - Improper Access Control in Users

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

Jack Anderson 9 months ago Maintainer

Hi Faisal,

The Security Team have now assessed the following issue:

SCRMBT-#189 - Improper Access Control in Users

This issue has been given a severity grading of 'Important'. Due to the severity 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 included or have a specific request on how you would like to be referenced within the release notes.

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

Faisal Fs ⚔️ 9 months ago Researcher

Great, thanks for the update. You can use the name in the release notes as

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

Thank you.

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 ✘

Sign in to join this conversation