# Improper Authorization in salesagility/suitecrm

0

Valid Reported on Feb 14th 2022

## Description

In SuiteCRM v7.12.4, affecting Employee Module, any user with the User Type as Regular User could export employee records via `/index.php?entryPoint=export` endpoint. The prerequisite of this attack is by knowing the user record (ID) which can be obtained in the employees' section. The impact could lead to employee record information exposure such as User Name, Full Name, ID, Full Address, Phone Number and others.

## Proof of Concept

Affected Endpoint:
1 POST http://{HOST}/index.php?entryPoint=export
~
Request file , pwd: `xBCwVicbq9`

## Impact

This vulnerability is capable of leading to unauthorized sensitive information disclosure of relevant parties such as User Name, ID and others that can be used to orchestrate the further attack.

## Occurrences

Employee.php?q=%22EMPLOYEES%22+++language%3APHP L187-L214

CVE
CVE-2022-0756
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by


Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

Matt Lorimer
@mattlorimer
maintainer

This report was seen 498 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

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-#190 - Improper Authorisation in Employees

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-#190 - Improper Authorisation in Employees

This issue has been given a severity grading of 'Moderate'. We will look to release a fix for this issue in the near future.

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.
Btw, you can use the name in the release notes as

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

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 ✖

**Employee.php?q=%22EMPLOYEES%22+++language%3APHP#L187-L214** has been validated ✔

Sign in to join this conversation

privacy policy

Chat with us