Improper access control could make any user export all user of website in humhub/humhub

1

Valid Reported on Apr 12th 2022

Description

A user who has to change their password after logging in can export the website's user data.

Proof of Concept

Step 1: login to website by admin account and change password of a user. Check the box "Force password change upon next login" and save.
Step 2: login to website by the account you just change the password. You will see a change password page.
Step 3: go to the link: domain/admin/user/export?format=xlsx. You will see this account can export the data of users without admin privilege.
You may try it out on ncsctest.humhub.com, which is my demo site. After logging in, a user tester / 123123 will be forced to change their password. You can view the export file humhub user.xlsx at https://ncsctest.humhub.com/admin/user/export?format=xlsx.

Impact

As a result, the attacker may be able to acquire data from all users on the website.

Occurrences

ControllerAccess.php L231-L350

CVE
CVE-2022-24865
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Critical (9.1)

Registry
Other

Affected Version
1.10.3

Visibility
Public

Status
Fixed

Found by

lekhang123lc
@lekhang123lc
unranked

This report was seen 683 times.

We are processing your report and will contact the **humhub** team within 24 hours. 7 months ago

We have contacted a member of the **humhub** team and are waiting to hear back 7 months ago

Lucas 7 months ago Maintainer

Thanks for the report. We can confirm the error and are working on a solution.

A **humhub/humhub** maintainer has acknowledged this report 7 months ago

Lucas Bartholemy validated this vulnerability 7 months ago

lekhang123lc has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **humhub** team. We will try again in 7 day

Lucas Bartholemy marked this as fixed in 1.9.4 & 1.10.4 & 1.11.0 with commit eb83de
7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

ControllerAccess.php#L231-L350 has been validated ✔

Lucas 7 months ago Maintainer

CVE-2022-24865

Sign in to join this conversation