Exposure of Sensitive Information to an Unauthorized Actor in snipe/snipe-it

2

Valid Reported on Feb 11th 2022

Description

An attacker can enumerate users through the response message in the password reset page. When you visit the password reset page, you will be provided with the option to enter your email address. Let's use two different emails, one will be a valid address, and another will be an invalid one.

Reproduction

When you enter the first email address and submit the form, you will get a HTTP response, where it says: "*Success: Your password link has been sent!*".
Now, when you enter the second email address and submit the form, the HTTP response will contain: "*Success: If that email address exists in our system, a password recovery email has been sent.*"
Here, you can clearly see that there are two different response messages. By analyzing these responses, it is clear that an attacker can determine which email addresses are registered in this portal, and which aren't.

Impact

An attacker would be able to increase the probability of success of password brute-forcing attacks against the system, because he/she would be able to figure out which email addresses they need to try their brute-forcing attacks on.

How to Fix

This vulnerability can be fixed by providing a response like "*Success: If that email address exists in our system, a password recovery email has been sent.*" for valid email addressess as well.

Occurrences

passwords.php L4

Fine: https://github.com/snipe/snipe-it/blob/master/resources/lang/en/auth/message.php#L34-L42
To change: https://github.com/snipe/snipe-it/blob/master/resources/lang/en/passwords.php#L4

References

- WSTG - Testing for Account Enumeration and Guessable User Account

CVE
CVE-2022-0569
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Binit Ghimire
@thebinitghimire
unranked

Fixed by

Binit Ghimire
@thebinitghimire
unranked

We are processing your report and will contact the **snipe/snipe-it** team within 24 hours.
9 months ago

Binit Ghimire submitted a patch 9 months ago

Binit Ghimire 9 months ago Researcher

In the patch, I have made changes to the English language strings. Please make similar changes for other internationalized files!

snipe validated this vulnerability 9 months ago

Binit Ghimire has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

snipe marked this as fixed in **v5.3.9** with commit **05c081** 9 months ago

Binit Ghimire has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

passwords.php#L4 has been validated ✔

Sign in to join this conversation