Generation of Error Message Containing Sensitive Information in snipe/snipe-it

1

Valid Reported on Feb 11th 2022

Description

An attacker can enumerate users through the response time 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.
When you enter the first email address and submit the form, you will get a HTTP response within a certain period of time. Let’s suppose this is 5 seconds.
Now, when you enter the second email address and submit the form, you will get a HTTP response within a certain period of time, which is always less than the time taken by the first email address. Let's suppose this is 2 seconds.

Cause

This behavior is shown, because the backend server possibly performs the following actions:
Check whether the email address exists in the database,
If it doesn’t exist, then throw a response immediately.
If it exists, perform further processing, to send a reset email, possibly a SMTP request, then throw a response.
Actually, this is the behavior of the majority of the applications, however in case of this application, the response time varies every time, i.e. the process is happening one after the other instead of doing the email sending part in the background.
By analyzing this behavior, an attacker can easily determine which email addresses exist in the database, and which don’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 they need to try their brute-forcing attacks on.

Occurrences

ForgotPasswordController.php L68-L95

References

- WSTG - Testing for Account Enumeration and Guessable User Account

CVE
CVE-2022-0622
(Published)

Vulnerability Type
CWE-209: Generation of Error Message Containing Sensitive Information

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Binit Ghimire
@thebinitghimire
unranked

Fixed by

snipe
@snipe
maintainer

This report was seen 460 times.

We are processing your report and will contact the **snipe/snipe-it** team wit
9 months ago

Chat with us

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back
9 months ago

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

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 **5.3.11** with commit **178e44** 9 months ago

snipe has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

ForgotPasswordController.php#L68-L95 has been validated ✅

Sign in to join this conversation

terms

privacy policy

Chat with us