Old sessions are not blocked by the login enable function. in snipe/snipe-it

0

Valid Reported on Mar 25th 2022

Description

If you disable logic function of an user, that user can still login by using their old session.

Proof of Concept

Step 1: login to dashboard by a normal account.
Step 2: use a diffrent browser to login as admin
Step 3: make the normal account in step 1 unable to login.
Step 4: return to the browser login the normal account and refresh. You can see that this user can still login and use website's feature like create asset (if this account has permission)

Impact

This could make leaked data.

Occurrences

UsersController.php L210-L308

CVE
CVE-2022-1155
(Published)

Vulnerability Type
CWE-840: Business Logic Errors

Severity
High (7.4)

Visibility
Public

Public

Status
Fixed

Found by

lekhang123lc
@lekhang123lc
unranked

Fixed by

snipe
@snipe
maintainer

This report was seen 720 times.

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

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

We have sent a follow up to the **snipe/snipe-it** team. We will try again in 7 days. 8 months ago

snipe validated this vulnerability 8 months ago

lekhang123lc has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

snipe marked this as fixed in **5.3.10** with commit **bdabbb** 8 months ago

snipe has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

UsersController.php#L210-L308 has been validated ✔

Sign in to join this conversation

Chat with us