huntr

Improper Access Control in snipe/snipe-it

0

✓ Valid Reported on Jan 9th 2022

Description

A user with no rights for API tokens can view the page where API tokens can be generated and can generate API tokens.

Proof of Concept

Create a user with no permission for anything (i.e. everything on deny).
Log in with this user to the web application.
Visit `http://127.0.0.1:8000/account/api` => The user can see and generate personal API tokens even the user has no rights for it.

Impact

The impact trends to be low as the user sees / generates his own API tokens. If the page would have some other serious errors, the attacker could from this point on doing more stuff.

Occurrences

ProfileController.php L116

There is no check that the user cannot view that site if no permission is given.

CVE
CVE-2022-0178
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity

Severity

Medium (6.3)

Visibility

Public

Status

Fixed

Found by

starkitsec

@starkitsec

unranked

Fixed by

snipe

@snipe

maintainer

This report was seen 367 times.

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

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

snipe validated this vulnerability a year ago

starkitsec has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

snipe a year ago Maintainer

This is very low impact, since a user wth no permissions to do anything would create an API user with no permissions to do anything, since the API token inherits the permissions from the user who created it, but it's a valid bug. I'll have a fix out this week.

snipe a year ago

(Thank you for the report btw)

snipe marked this as fixed in **5.3.8** with commit **0e5ef5** 10 months ago

snipe has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ProfileController.php#L116 has been validated ✓

Sign in to join this conversation