

Improper Privilege Management in snipe/snipe-it

2

✓ Valid

Reported on Feb 11th 2022

Description

It was found that if a user is not having access to supplier module, he can access and view the supplier content.

Proof of Concept

Create two users, one admin and one normal user

A normal user is not having access to the supplier module.

But by enumeration the normal user view the restricted content of supplier by enumeration.

POC

<https://demo.snipeitapp.com/suppliers/1> Just enumerate the number, and you will see the details

Impact

This vulnerability will help an attacker view restricted content.

CVE

CVE-2022-0579

(Published)

Vulnerability Type

CWE-269: Improper Privilege Management

Severity

Medium (6.5)

Visibility

Public

Status

Fixed

Chat with us

Found by

**shubh123-tri**

@shubh123-tri

unranked ▾

Fixed by

**snipe**

@snipe

maintainer

This report was seen 390 times.

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

10 months ago

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

9 months ago

snipe validated this vulnerability 9 months ago

shubh123-tri has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

snipe marked this as fixed in **5.3.9** with commit **db0c0e** 9 months ago

snipe has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

[Chat with us](#)