huntr

Improper Access Control in snipe/snipe-it

0

✓ Valid Reported on Jan 5th 2022

Description

All bulk actions (bulk-edit / bulk-delete / form info) in asset models do not have access control checks

Proof of concept

1: Grant view to Asset Models
2: UI for bulk-edit and bulk-delete is still enabled, proceed.
3: You may bulk-delete / edit any asset model

Impact

This vulnerability is capable of viewing / editing / delete asset model information with DENY permissions,

CVE
CVE-2022-0179
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (6.3)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron

@haxatron

pro

Fixed by

haxatron

@haxatron

pro

This report was seen 414 times.

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

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron submitted a patch a year ago

haxatron submitted a patch a year ago

haxatron a year ago Researcher

Fix commit: https://github.com/Haxatron/snipe-it/commit/bb095641c2f421f744796d184287c46fc9303591

Let me know if you want a PR :)

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

haxatron modified the report a year ago

haxatron a year ago

note that fix is on master branch, not fix-access-control branch, also updated permalinks to reflect where all 4 issues occur reflect where all 4 issues occur

haxatron modified the report a year ago

haxatron modified the report a year ago

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

snipe a year ago Maintainer

You are a rock star <3 - can you PR this? It would be easier for me - if you can't, no worries, I'll sort it out.

haxatron a year ago Researcher

Done - https://github.com/snipe/snipe-it/pull/10498

haxatron a year ago Researcher

@maintainer, could you validate this? Thanks! :D

snipe validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

snipe a year ago Maintainer

Done,, and thanks :) You can call me snipe ;)

haxatron a year ago Researcher

No problem snipe, happy to contribute to the security of your project. Once a new release is available, or when you are comfortable, could you submit the fix for this as well? That would be great! :)

snipe marked this as fixed in **5.3.6** with commit **cf14a0** 10 months ago haxatron has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation