Cross-site Scripting (XSS) - Generic in snipe/snipe-it

0

Valid Reported on Nov 5th 2021

Description

XSS in bulk audit function via the asset tag parameter

Proof of Concept

```
1: Go to http://<SNIPE_IT_APP>/hardware/bulkaudit feature
2: Use <script>alert(document.domain)</script> as "Asset Tag" parameter
3: Click "Audit", the XSS should be triggered via the message Asset Tag [AS
```

Impact

This vulnerability is capable of tricking users without knowledge of XSS to key in the malicious payload and thus steal the cookie or perform actions on behalf of them via Javascript execution. Due to CSRF protections, I am unable to escalate this further but thought I should report to you just in case you care about it.

CVE
CVE-2021-3938
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Generic

Severity
Low (3.9)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

snipe
@snipe
maintainer

This report was seen 404 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

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

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

snipe marked this as fixed with commit **9ed144** a year ago

snipe has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

Sign in to join this conversation