Stored Cross Site Scripting vulnerability in Item name parameter in snipe/snipe-it

0

Valid Reported on Apr 11th 2022

Description

Stored cross site scripting vulnerability on Item name parameter in Assest module. Add payload in item name and whenever the user add the item in his requested assest . The alert will trigger.

Proof of Concept

Login to the demo account
Go to Asset functionality , add or edit an item name with following payload and save
payload = "><iMg SrC="x" oNeRRor="alert(1);">
Go to requested assets , check the item name (payload), that you added or edit an asset which are already in requested asset
If it is there, alert will be triggered

Impact

The vulnerability is capable of stolen the user Cookie.

CVE
CVE-2022-1380
(Published)

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

Severity
Critical (9.1)

Registry
Packagist

Affected Version

v5.4.1

Visibility
Public

Status
Fixed

Found by

Asura-N
@asura-n
noisy

Fixed by

snipe
@snipe
maintainer

This report was seen 693 times.

We are processing your report and will contact the **snipe/snipe-it** team within 24 hours. 8 months ago

Asura-N modified the report 8 months ago

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back 7 months ago

snipe 7 months ago Maintainer

I am unable to reproduce this. In the line cited, you can see the name is escaped using the `e()` escaping syntax.

snipe 7 months ago Maintainer

https://demo.snipeitapp.com/hardware/requested (the demo resets, so I don't know if the test will still be there when you check this message.)

Asura-N 7 months ago Researcher

HI snipe , it is still executing, I will share vedio poc in a while for clear understanding

Thanks
Asura-N

Asura-N 7 months ago — Researcher

https://mega.nz/file/A8knDSjY#gCZggqdSnnVX0N_VN6RPRIB00DB4xFI3Ogwwc-Icl20

snipe 7 months ago — Maintainer

Thanks Asura - I am away for the day but will check when I return.

snipe 7 months ago — Maintainer

Got it - this is on the *user's* requested assets page, not the admin's.

snipe validated this vulnerability 7 months ago

Asura-N has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

snipe marked this as fixed in **v5.4.3** with commit **f211c1** 7 months ago

snipe has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation