huntr

Stored XSS in Part Description in inventree/inventree

0

✓ Valid Reported on Jun 11th 2022

Description

The application `inventree` is vulnerable to Stored XSS in part description field.

Proof of Concept

Video PoC link:
https://drive.google.com/file/d/1ZFgWiVpalxZ8zGeDrErezjZCQjB3VP-w/view?usp=sharing

Impact

This allows the attacker to execute malicious scripts in all the project members browser and it can lead to session hijacking, sensitive data exposure, and worse.

CVE
CVE-2022-2113
(Published)

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

Severity
High (8.4)

Registry
Pypi

Affected Version
0.7.1

Visibility
Public

Status
Fixed

Chat with us

Found by

saharshtapi

@saharshtapi

master

Fixed by

Oliver

@schrodingersgat

maintainer

This report was seen 596 times.

We are processing your report and will contact the **inventree** team within 24 hours.
6 months ago

saharshtapi modified the report 6 months ago

Matthias Mair modified the Severity from Critical (9) to High (8.4) 5 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Matthias Mair validated this vulnerability 5 months ago

This is a valid vulnerability - it will be fixed within 28 days by the maintainers.

saharshtapi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Oliver marked this as fixed in **0.7.2** with commit **26bf51** 5 months ago

Oliver has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

saharshtapi 5 months ago Researcher

@admin Can you assign CVE?

saharshtapi 5 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 5 months ago Admin

CVE assigned 👏

> Sign in to join this conversation