Unrestricted File Upload in Part Attachment in inventree/inventree

2

Valid Reported on Jun 11th 2022

Description

The application `inventree` allows users to upload any file in part attachment allowing attacker to render files such as HTML in the browser.

Proof of Concept

Video PoC Link:
https://drive.google.com/file/d/1vurBkHegeYCwbXopE5Yhyb702rYgG9FM/view?usp=sharing

Impact

Authenticated user can upload dangerous file to anywhere in server (example: upload a file with .html extension lead to stored xss)

References

- nvd

CVE
CVE-2022-2111
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9)

Registry
Pypi

Affected Version

0.7.1

Visibility
Public

Status
Fixed

Found by

saharshtapi
@saharshtapi
master

Fixed by

Oliver
@schrodingersgat
maintainer

This report was seen 647 times.

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

Matthias Mair 5 months ago Maintainer

As of now, this is intended. Any file can be added by authorized users. I will discuss this with the team and then we will decide how to classify this.

Matthias Mair has marked this vulnerability as informative 5 months ago

Hi there @saharshtapi . The dev team decided this is expected behaviour. We will add notes to our docs and maybe the ui and thank you for your consideration. It is a core workflow to upload html test reports via the api so we can not cut this option.

The disclosure bounty has been dropped ×

The fix bounty has been dropped ×

The researcher's credibility has not been affected

saharshtapi 5 months ago Researcher

I totally understand but a better practice would be do download the file on clicking the link rather than opening in the browser using the servers URL. Doing this will prevent any kind of XSS attack which can allow an attack to change privileges or other harmful scenarios, as the file will be getting downloaded.

Oliver 5 months ago Maintainer

@saharshtapi a very good point and I will issue a fix to ensure files are downloaded rather than opened directly in the browser.

saharshtapi 5 months ago Researcher

@maintainer can you please valid this report as you can see my perspective now as many applications also face the similar issue and I think I can ask this much in return 😃🦾.

Matthias Mair 5 months ago Maintainer

We are working on that - it seems to be a manual process to change that.

Jamie Slome 5 months ago Admin

I've reopened the report for you ♥ Feel free to proceed as you wish @maintainer!

Oliver validated this vulnerability 5 months ago

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 ✘

This vulnerability will not receive a CVE ❌

Matthias Mair 5 months ago Maintainer

@saharshtapi sorry for the delay and thank you for suggesting the fix we didn't think about before!

saharshtapi 5 months ago Researcher

@maintainer great work on fixing all the bugs in such a short time. 🎉 🍾

Matthias Mair 5 months ago Maintainer

@sarahstapi we try to keep our users safe - if the community keeps reporting we will keep fixing ;-). All XSS reports were caused by the same error so the fix by @Oliver was released in under 1 day after we decided it was an issue.

saharshtapi 5 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 5 months ago Admin

Before we proceed with CVEs for each of the reports, we first require the permission of the maintainer 👍

@maintainer - are you happy for us to assign and publish CVEs for each of the recent valid reports?

Oliver 5 months ago Maintainer

All confirmed reports have now been patched and published here - https://github.com/inventree/InvenTree/security/advisories?state=published

So yes, we are happy for these to be made public now

Jamie Slome 5 months ago

That is great - shall I proceed with a CVE for each valid and public report? A CVE is good practice

and allows users of your software to know about the vulnerability in a responsible way :)

Oliver 5 months ago Maintainer

Please do!

saharshtapi 5 months ago Researcher

Thank you @oliver!!

Jamie Slome 5 months ago Admin

CVE assigned: `CVE-2022-2111`

It should be published shortly too 👏 Feel free to update the relevant GitHub Security Advisory with the CVE number stated above.

Matthias Mair 5 months ago Maintainer

Sorry if I am coming in late herebut all the XSS reportsare the exact same issue and fix - that should be only 1 CVE right?

saharshtapi 5 months ago Researcher

Looking at other application's reports and cve database the cve's were assigned to all XSS.

Jamie Slome 5 months ago Admin

Because I facilitated this manually, we have only allotted one CVE for all of the XSS issues, as they only required a single fix to address all of the issues 👍

saharshtapi 5 months ago Researcher

Understood!!

Matthias Mair 5 months ago

@admin thank you for the response. I was not sure if this is automated and might lead to spam in the CVE database- which might not be good.

Sign in to join this conversation