The NocoDB application allows large characters to insert in the input field "New Project" on the create field which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request in nocodb/nocodb

0

✓ Valid Reported on Jun 16th 2022

Proof of Concept

Go to http://localhost:8080/dashboard/#/projects Click on New project and create Fill the "Enter project name" field with huge characters, (more than 1 lakh) Copy the below payload and put it in the input fields and click on continue. You will see the application accepts large characters and if we will increase the characters then it can lead to Dos.

Download the payload from here:

https://drive.google.com/file/d/13IK67Sx93nvnb_3gLUBDLgoEC7XTQiso/view?usp=sharing

Video & Image POC:

https://drive.google.com/drive/folders/1N6h02blexPhQyj4MdfyPwNTOmKEXIfMu?usp=sharing

Patch recommendation:

The Project name input should be limited to 50 characters or a max of 100 characters.

Impact

It can lead to a denial of service attack

References

- https://huntr.dev/bounties/cdf00e14-38a7-4b6b-9bb4-3a71bf24e436/
- https://huntr.dev/bounties/97e36678-11cf-42c6-889c-892d415d9f9e/

CVE

CVE-2022-3423
(Published)

Vulnerability Type

CWE-400: Denial of Service

Severity

High (7.3)

Registry

Other

Affected Version

0.91.10

Visibility

Public

Status

Fixed

Found by

Arjun E

@hisokix0

master

This report was seen 570 times.

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

Arjun E modified the report 5 months ago

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

A **nocodb/nocodb** maintainer 5 months ago

Maintainer

Handled in below PR image.

```
docker run -d -p 8888:8080 nocodb/nocodb-timely:0.91.10-pr-2416-2022
```

Chat with us

Expected to be available in the next release.

♥ navi gave praise 5 months ago

Thank you for the report - we are looking debugging the issue

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

We have sent a follow up to the **nocodb** team. We will try again in 7 days. 5 months ago

A **nocodb/nocodb** maintainer has acknowledged this report 5 months ago

Arjun E 5 months ago Researcher

Any updates?

A **nocodb/nocodb** maintainer validated this vulnerability 5 months ago

Arjun E has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **nocodb/nocodb** maintainer marked this as fixed in **0.92.0** with commit **000ecd** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Arjun E 5 months ago Researcher

@admin am I eligible to assign a CVE?

Jamie Slome 5 months ago Admin

We are happy to assign and publish a CVE if the maintainer is happy to do so

Chat with us

@maintainer - are you happy with a CVE for this report?

@maintainer - are you happy with a CVE for this report?

Arjun E 4 months ago Researcher

@maintainer - Any updates from your side ?

wingkwong 2 months ago Maintainer

The fix has been deployed. You may assign & publish a CVE.

Arjun E 2 months ago Researcher

@admin - maintainer is happy to assign the CVE, Please approve the CVE id @admin

Ben Harvie 2 months ago Admin

I have started the CVE assignment process and it should be published shortly. Happy hunting:)

Sign in to join this conversation