Insufficient Session Expiration in nocodb/nocodb

0

Valid Reported on Jun 3rd 2022

Description

The application NocoDB failed to invalidate the session after changing the password and In this scenario changing the password doesn't destroy the other sessions which are logged in with old passwords.

Proof of Concept

```
Login same account in two different browsers.

Try to change the password from browser one.

You will see after changing the password, sessions don't get destroyed from
```

poc video

https://drive.google.com/file/d/1gFn8BLktl90v2YfIRTimvFgu2rhNWoTx/view?usp=sharing

Impact

If a user's account got compromised and he/she tried to change the password still after changing the password session will not destroy and the attacker will have control over the account.

References

- CVE-2020-35358

CVE-2022-2064
(Published)

Vulnerability Type
CWE-613: Insufficient Session Expiration

Severity
Critical (9.1)

Registry
Npm

Affected Version
0.91.7

Visibility
Public

Status
Fixed

Found by

Raj
@rajbabai8
master

Fixed by

navi
@o1lab
maintainer

This report was seen 454 times.

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

Raj 6 months ago Researcher

Hello @admin the maintainer has provided the email id so can you pls invite them to this report

We have contacted a member of the **nocodb** team and are waiting to hear

Jamie Slome 6 months ago Admin

Sorted 👍

Raj modified the report 6 months ago

We have sent a follow up to the **nocodb** team. We will try again in 7 days. 6 months ago

navi validated this vulnerability 5 months ago

Raj has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

navi marked this as fixed in **0.91.7+** with commit **c9b511** 5 months ago

navi has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation