

[\(/submissions\)](#)[\(/workflows\)](#) [Go back](#)

## Information Disclosure on Github

Submitted at

Submitted almost 2 years ago

Last activity

Last activity almost 2 years ago

## Status

Not applicableDuplicate

This submission was marked not applicable. It is not a rewardable submission at this time.

## Reward

version

[1.12 \(/vulnerability-rating-taxonomy/1.12\)](#)

## Engagement

Submitted to

[Immutable Bug Bounty \(/engagements/immutable\)](#)

## Closed on

20 Feb 2024

## CrowdStream visibility

Choose to show your details with this submission in CrowdStream when accepted.

Support

Please note: your username will always be shown with your submission if it is disclosed.

 Show username

Show reward

 **Please note:** This engagement does not currently disclose submission activity in CrowdStream.

[Submission details](/submissions/4870bcc5-4e9d-4d2a-8bda-e387ecc7ff66)(/submissions/4870bcc5-4e9d-4d2a-8bda-e387ecc7ff66)

## Revisions

[1 \(/submissions/4870bcc5-4e9d-4d2a-8bda-e387ecc7ff66/revisions\)](#)

## ID

4870bcc5-4e9d-4d2a-8bda-e387ecc7ff66

## Submitted

18 Feb 2024 02:09:13 GMT+5:30

## Target Location

## Target category

Unspecified

## VRT (VULNERABILITY RATING TAXONOMY)

Sensitive Data Exposure > Disclosure of Secrets > For Publicly Accessible Asset

## Priority

P1 Suggested priority based on the identified VRT

## Bug url

<https://github.com/NiluK/ethGlobal-game/blob/474897c32aebbf1a6760167a64d4b727fc087459/.env#L6>

## Description

Sensitive Token Exposed in GitHub

### Overview of the Vulnerability

There is an Exposure of tokens in the repositories of the given GitHub URL.

An attacker can use the credentials to access the privileges of the API Key owner and will be also able to make unauthorized requests.

### Steps to Reproduce

1. Go to the following repository:

<https://github.com/NiluK/ethGlobal-game/blob/474897c32aebbf1a6760167a64d4b727fc087459/.env#L6>

2. Here you can see the API Keys and Passwords .

## Impact

An attacker can access the Mongo Atlas Database as well as the Alchemy key is also exposed. Private Key is also exposed.

## Proof of Concept (PoC)

The following screenshot shows the sensitive token exposed:

## Files attached

 [PoC.png \(28.5 KB\) \(/attachments/kydjjgvvby\)](#)

## Disclose report to CrowdStream

Open a request to disclose this report to [CrowdStream \(/crowdstream\)](#). We recommend requesting disclosure after the vulnerability is marked as resolved.

Disclosure requests **will not speed up** submission transition.

Please review our [Public Disclosure Policy](#)

(<https://www.bugcrowd.com/resources/essentials/standard-disclosure-terms/>) before submitting a request.

## Activity

**SUDOxSatya** created the submission

almost 2 years ago (18 Feb 2024 02:09:13 GMT+5:30)

**momo\_bugcrowd** updated VRT to **Sensitive Data Exposure > Disclosure of Secrets > For Publicly Accessible Asset**

almost 2 years ago (20 Feb 2024 22:19:43 GMT+5:30)

**momo\_bugcrowd** changed the state to **Not applicable**

almost 2 years ago (20 Feb 2024 22:19:44 GMT+5:30)

**momo\_bugcrowd** marked the submission a duplicate of **Sensitive Information Disclosure** almost 2 years ago (20 Feb 2024 22:19:44 GMT+5:30)

 Sensitive Information Disclosure

VRT: For Publicly Accessible Asset

Target:

Submitted: 07 Oct 2023 21:15:27 IST

**momo\_bugcrowd** sent a message

almost 2 years ago (20 Feb 2024 22:19:52 GMT+5:30)

Hi SUDOxSatya,

Thank you for your submission. Unfortunately, we have received this report from another researcher. Therefore, it is considered a duplicate issue. Your effort is appreciated and we hope that you will continue to research and submit any future security issues you find.

If this is a paid program, points for this submission will be awarded when the submission that you're duplicated against moves to a final state, if the priority is P1 or P2. If that submission is marked as not applicable , or this submission is in a VDP (unpaid) program, then no points will be awarded as these aren't awarded on submissions of this state.

Best regards,

- mehmet\_bugcrowd

## Request a response

You can request a response from the customer or Bugcrowd about your submission. [Learn more.](#) (<https://docs.bugcrowd.com/researchers/reporting-managing-submissions/researchers-unread-comments/>)

[Submit a request](#)    2 of 2 available