







AWS secret key and NPM token leaked in MEW GitHub repos

State	 Triaged (Open)
Reported To	MyEtherWallet
Asset	www.myetherwallet.com (Domain)
Weakness	Insecure Storage of Sensitive Information
Severity	 Medium (4 ~ 6.9)
Participants	   
Visibility	Private

[Collapse](#)

TIMELINE · EXPORT

[near_](#) submitted a report to [MyEtherWallet](#).

Apr 27th (2 days ago)

Background

NPM tokens allow you to publish and access your modules on the NPM registry and give continuous integration tools access to your NPM packages: <https://docs.npmjs.com/about-authentication-tokens>

AWS secret keys can be used to sign requests that you make to AWS and "might give someone full access to your account" depending on the scope: <https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

An NPM token and AWS secret key pair were leaked in removed commits from the **MEWconnect-API-V2** and **MEWconnect-web-client** repos respectively.

Issue

NPM

Browse to <https://github.com/MyEtherWallet/MEWconnect-web-client/commit/1a44567d81f90850cd03bc7832e354d9df25f571#diff-c9ddf855a0f7d04bfc833074d20abf66L1> and observe that the NPM token is leaked in an "initial cleanup" commit.

NPM tokens can be used with the [CLI](#) and CI tools such as [Travis](#).

AWS

Browse to <https://github.com/MyEtherWallet/MEWconnect-API-V2/commit/33329528ba30b796283052dd6e8d61333f39c934> and observe that the AWS key pair is leaked in a "working example" commit.

The `aws_access_key_id` and `aws_secret_access_key` can be added to your "credentials" dot file and used to make AWS CLI requests: <https://docs.aws.amazon.com/cli/latest/index.html>

```
[repro]
aws_access_key_id=AKIAJPC5ZTPL0I6YAYJA
aws_secret_access_key=074EBmFGA28UCgeh+XhkGXNVW8F0wdUNzXhdYvpm
```

For instance, an attacker could list the S3 buckets scoped to the MEW AWS token:

```
$ aws s3 ls --profile repro
2017-07-19 16:32:32 myflixcdn
2017-07-19 16:32:14 myflixingest
2019-01-08 22:27:04 simple-chat-test
```

Impact

I have not made any further API calls with the leaked AWS key (besides the single example in the PoC), and have not made any calls with the NPM token, but assume both provide some level of privileged access to MEW dev environments per the "Background" section.



bassguitar HackerOne staff changed the status to Triaged.

Apr 28th (about 1 day ago)

Hello @near_

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
@bassguitar



olchik posted a comment.

Apr 29th (16 hrs ago)

Hi @near_ ,

Thank you for your report. We are looking in to this right now. As of right now, it seems that the AWS key is for the test environment. We will get back to you soon.

Thanks.



emperor joined this report as a participant.

Apr 29th (4 mins ago)



Add a comment...

Parsed with [Markdown](#)

Drag & drop or [select more files from your computer](#) (max. 250MB per file)

Post comment