Authorization Bypass Through User-Controlled Key in unshiftio/url-parse

3

Valid Reported on Jan 7th 2022

Description

Improperly handeling username and password . And unable to detect the hostname .

Proof of Concept

url-parse not able verify basic authentication credential and also wrongly verifying hostname .This allow to bypass hostname validation .
Lets username is `admin` and password is `password123@` and hostname is `127.0.0.1` .
so the url will be `http://admin:password123@@127.0.0.1` .
And there is blacklist check for domain `127.0.0.1` and every request to `127.0.0.1` will be blocked .\
Now lets use url-parse

```
// PoC.js
 var parse = require('url-parse')
var cc=parse("http://admin:password123@@127.0.0.1")
```

result

```
{ slashes: true,
  protocol: 'http:',
  hash: '',
  query: '',
  pathname: '/',
  auth: 'admin:password123',
  host: '@127.0.0.1',
  port: '',
  hostname: '@127.0.0.1',
```

```
    password: 'password123',
    username: 'admin',


    origin: 'http://@127.0.0.1',
    href: 'http://admin:password123@@127.0.0.1/' }
```

Here see its incorrretly detecting `auth` , `origin` , `password` and `hostname` .
Here hostname check `cc.hostname` is `@127.0.0.1` and also `cc.origin` is `http://@127.0.0.1` which will clearly bypass above `127.0.0.1` blacklist check .
Now if you use `cc.href` to fetch url then it will fetch `127.0.0.1` .

Impact

Bypass hostname check

Occurrences

JS index.js L17-L540

CVE
CVE-2022-0512
(Published)

Vulnerability Type
CWE-639: Authorization Bypass Through User-Controlled Key

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

Luigi Pinca

@lpinca

maintainer

This report was seen 1,097 times.

We are processing your report and will contact the **unshiftio/url-parse** team within 24 hours.
a year ago

We have contacted a member of the **unshiftio/url-parse** team and are waiting to hear back
a year ago

Luigi Pinca a year ago Maintainer

@3rd-eden I think this is valid. I've opened a PR with a possible fix https://github.com/unshiftio/url-parse/pull/223.

ranjit-git a year ago Researcher

can you plz mark this report as valid ?

Luigi Pinca a year ago Maintainer

Waiting for @3rd-eden. I can't publish a new version on npm and I would prefer to have a CVE only after a new version is published.

ranjit-git a year ago Researcher

Ok, got it

We have sent a follow up to the **unshiftio/url-parse** team. We will try again in 7 days.
10 months ago

We have sent a second follow up to the **unshiftio/url-parse** team. We will try again in 10 days.
10 months ago

ranjit-git 10 months ago Researcher

hello, any update?

ranjit-git 10 months ago Researcher

can you plz validate the report ?

Luigi Pinca 10 months ago Maintainer

Please be patient. @3rd-eden is not responding. I've already contacted a maintainer that can publish to npm.

Jamie Slome 10 months ago Admin

@ranjit-git - please allow the maintainers the time they require to follow up on addressing any vulnerabilities and publishing fixes.

@luigi - if you would like a delay before publishing the CVE, please confirm the fix once you are ready for both the report and CVE to go public.

Let me know if you have any more questions and more than happy to assist.

ranjit-git 10 months ago Researcher

oh, sorry
i should have re-check the PR url you provided above https://github.com/unshiftio/url-parse/pull/223 is still pending .
Take your time , no problem

Luigi Pinca 10 months ago Maintainer

@admin please add https://github.com/Swaagie as a maintainer.

Jamie Slome 10 months ago Admin

@luigi - if they just visit the URL for this report whilst logged in, and they have repository write permissions, they will be given access to the repository and all future reports.

Let me know how this goes, otherwise, I will add them manually on my side once they have signed up 👍

signed up 👍

Luigi Pinca 10 months ago Maintainer

Ok, yes, they have full administrator access.

Jamie Slome 10 months ago Admin

Great, let me know if they are struggling to view the page once signed up ♥

We have sent a third and final follow up to the **unshiftio/url-parse** team. This report is now considered stale. 10 months ago

Jamie Slome 10 months ago Admin

Any updates or support we can offer here @Luigi? Just checking @3rd-eden was able to view the report 👍

Luigi Pinca 10 months ago Maintainer

Still waiting... @3rd-eden can view but does not respond. @Swaagie told me that they will soon look into this.

Jamie Slome 10 months ago Admin

Thanks for the update Luigi!

Jamie Slome 10 months ago Admin

Looks like Swaagie has approved a potential fix here.

Are we able to confirm the report status as approved or rejected? If a CVE is assigned, it will not be published until a fix has been confirmed. This is the same with the visibility of the report.

Luigi Pinca validated this vulnerability 10 months ago

ranjit-git has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The fix bounty is now up for grabs

Jamie Slome 10 months ago Admin

Thanks Luigi!

The CVE has been added to the report, but will not be published - just to be extra explicit here ♥

We have sent a fix follow up to the **unshiftio/url-parse** team. We will try again in 7 days.
10 months ago

Luigi Pinca marked this as fixed in **1.5.6** with commit **9be7ee** 9 months ago

Luigi Pinca has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

index.js#L17-L540 has been validated ✔

Luigi Pinca 9 months ago Maintainer

@admin I've received an email with this text "3 days have elapsed since validating the report in unshiftio/url-parse. This is a reminder to ask you to confirm a fix against the report.".

I've already confirmed the fix 4 days ago.

Jamie Slome 9 months ago Admin

@lpinca - many apologies for this - this certainly looks like a bug on our side. I have stopped the e-mailing process, so no further e-mails should be received about this report.

We will take a deep dive into what happened here, and I will keep you updated on a fix.

Jamie Slome 9 months ago Admin

@lpinca - we have tracked down the bug and have released a patch for this. We will keep an eye on the e-mailing system, but please let us know if you still experience any unexpected or unsolicited e-mails.

Thanks for your support! 👍

ranjit-git 9 months ago Researcher

@maintainer
if a given url parsed as bellow by url-parse

```
{ slashes: true,
  protocol: 'http:',
  hash: '',
  query: '',
  pathname: '/',
  auth: '',
  host: 'example.com:22',
  port: '',
  hostname: 'example.com:22',
  password: '',
  username: '',
  origin: 'http://example.com:22',
  href: 'http://example.com:22/' }
```

is this consider to be a security bug here because hostname is different here with port which may bypass hostname check?

Luigi Pinca 9 months ago Maintainer

No, the hostname is invalid. The library might return invalid hostnames. This is documented. It is user responsibility to validate the hostname before doing any check against it.

Sign in to join this conversation