## huntr

# Authorization Bypass Through User-Controlled Key in medialize/uri.js

✓ Valid ) Reported on Feb 14th 2022

# Description

Bypass for https://huntr.dev/bounties/1625558772840-medialize/URI.js/

urijs fixed the issue for CVE-2021-3647, however an attacker can still exploit the issue due to case-sensitive checks in the earlier patch. Attacker can use case-insensitive protocol schemes like HTTP, http, etc. in order to bypass the patch for that bug.

# **Proof of Concept**

```
var URI = require('urijs');
var url = new URI("HTTPS:///github.com/abc");
console.log(url);
```

#### **OUTPUT:**

```
URI {
  string: '',
  parts: {
    protocol: 'HTTPS',
    username: null,
    password: null,
    hostname: null,
    urn: null,
    port: null,
    path: '/github.com/abc',
    query: null,
    fragment: null,
    preventInvalidHostname: false,
    duplicateQueryParameters: false,
```

Chat with us

```
escapeQuerySpace: true
},

_deferred_build: true
}
```

## **Impact**

Bypass host-validation checks, open redirect, SSRF etc. - depends on the usage of urijs

### Occurrences

JS URI.js L516

add i modifier for case-insensitive checks

#### CVE

CVE-2022-0613 (Published)

#### Vulnerability Type

CWE-639: Authorization Bypass Through User-Controlled Key

#### Severity

Medium (5.3)

#### Visibility

Public

#### Status

Fixed

#### Found by

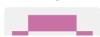


### Rohan Sharma

@r0hansl

unranked V

#### Fixed by



Rohan Sharma

Chat with us



This report was seen 615 times

We are processing your report and will contact the **medialize/uri.js** team within 24 hours. 9 months ago

Rohan Sharma submitted a patch 9 months ago

Rohan Sharma 9 months ago

Researcher

Submitted the patch and

PR: https://github.com/medialize/URI.js/pull/412

Rodney Rehm validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

Rodney Rehm 9 months ago

Maintainer

The fix provided by @r0hansh has been published as version 1.19.8 - https://github.com/medialize/URI.js/releases/tag/v1.19.8

Rodney Rehm marked this as fixed in 1.19.8 with commit 6ea641 9 months ago

Rohan Sharma has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

URI.js#L516 has been validated ✓

Sign in to join this conversation

Chat with us

#### 2022 © 418sec

### huntr

home

hacktivity

leaderboard

FAO

contact us

terms

privacy policy

## part of 418sec

company

about

team