huntr

Protocol/Hostname spoofing via Improper Input Validation in medialize/uri.js

2

✓ Valid Reported on Feb 26th 2022

Description

The uri.js doesn't remove whitespace characters from the beginning of the protocol, so it doesn't parse URLs properly. Several methods, including `http.get()` , `location.href` , and `fetch()` , strip the whitespace character in front of the protocol before sending the request.

Proof of Concept

```
const url = require('urijs');
console.log(new url("\bhttp://google.com"))
// console.log(new url("\bjavascript:alert(1)"))
```

output

```
URI {
  _string: '',
  _parts: {
    protocol: undefined,
    username: null,
    password: null,
    hostname: null,
    urn: null,
    port: null,
    path: '\bhttp://google.com',
    query: null,
    fragment: null,
    preventInvalidHostname: false,
    duplicateQueryParameters: false,
    escapeQuerySpace: true
  },
  _deferred_build: true
}
```

Mitigation

```
function remove_whitespace(url){
     const whitespace = /^[\x00-\x20\u00a0\u1680\u2000-\u200a\u2028\u2029\u
     url = url.replace(whitespace, '')
     return url
}
```

Write and use a function to remove white space characters as above.

CVE
CVE-2022-24723
(Published)

Vulnerability Type
CWE-20: Improper Input Validation

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

Pocas
@p0cas
amateur

This report was seen 1,027 times.

We are processing your report and will contact the **medialize/uri.js** team wi

9 months ago

Chat with us

Pocas modified the report 9 months ago

Pocas 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

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

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Rodney Rehm marked this as fixed in **1.19.9** with commit **86d105** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Rodney Rehm 9 months ago Maintainer

https://github.com/medialize/URI.js/releases/tag/v1.19.9 contains the fix, thanks for the report!

Sign in to join this conversation