

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



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
  }
}
```

[Chat with us](#)

```
},
  _deferred_build: true
}
```

Mitigation

```
function remove_whitespace(url){
    const whitespace = /^[\\x00-\\x20\\u00a0\\u1680\\u2000-\\u200a\\u2028\\u2029\\u2001-\\u200f\\u2013\\u2014\\u2018\\u2019\\u201c\\u201d\\u201e\\u201f\\u2020\\u2021\\u2022\\u2023\\u2024\\u2025\\u2026\\u2027\\u2028\\u2029\\u2030\\u2031\\u2032\\u2033\\u2034\\u2035\\u2036\\u2037\\u2038\\u2039\\u203a\\u203b\\u203c\\u203d\\u203e\\u203f\\u2040\\u2041\\u2042\\u2043\\u2044\\u2045\\u2046\\u2047\\u2048\\u2049\\u204a\\u204b\\u204c\\u204d\\u204e\\u204f\\u2050\\u2051\\u2052\\u2053\\u2054\\u2055\\u2056\\u2057\\u2058\\u2059\\u205a\\u205b\\u205c\\u205d\\u205e\\u205f\\u2060\\u2061\\u2062\\u2063\\u2064\\u2065\\u2066\\u2067\\u2068\\u2069\\u206a\\u206b\\u206c\\u206d\\u206e\\u206f\\u2070\\u2071\\u2072\\u2073\\u2074\\u2075\\u2076\\u2077\\u2078\\u2079\\u207a\\u207b\\u207c\\u207d\\u207e\\u207f\\u2080\\u2081\\u2082\\u2083\\u2084\\u2085\\u2086\\u2087\\u2088\\u2089\\u208a\\u208b\\u208c\\u208d\\u208e\\u208f\\u2090\\u2091\\u2092\\u2093\\u2094\\u2095\\u2096\\u2097\\u2098\\u2099\\u209a\\u209b\\u209c\\u209d\\u209e\\u209f\\u20a0\\u20a1\\u20a2\\u20a3\\u20a4\\u20a5\\u20a6\\u20a7\\u20a8\\u20a9\\u20aa\\u20ab\\u20ac\\u20ad\\u20ae\\u20af\\u20b0\\u20b1\\u20b2\\u20b3\\u20b4\\u20b5\\u20b6\\u20b7\\u20b8\\u20b9\\u20ba\\u20bb\\u20bc\\u20bd\\u20be\\u20bf\\u20c0\\u20c1\\u20c2\\u20c3\\u20c4\\u20c5\\u20c6\\u20c7\\u20c8\\u20c9\\u20ca\\u20cb\\u20cc\\u20cd\\u20ce\\u20cf\\u20d0\\u20d1\\u20d2\\u20d3\\u20d4\\u20d5\\u20d6\\u20d7\\u20d8\\u20d9\\u20da\\u20db\\u20dc\\u20dd\\u20de\\u20df\\u20e0\\u20e1\\u20e2\\u20e3\\u20e4\\u20e5\\u20e6\\u20e7\\u20e8\\u20e9\\u20ea\\u20eb\\u20ec\\u20ed\\u20ee\\u20ef\\u20f0\\u20f1\\u20f2\\u20f3\\u20f4\\u20f5\\u20f6\\u20f7\\u20f8\\u20f9\\u20fa\\u20fb\\u20fc\\u20fd\\u20fe\\u20ff\\u2000-\\u20ff\\u2100-\\u21ff\\u2200-\\u22ff\\u2300-\\u23ff\\u2400-\\u24ff\\u2500-\\u25ff\\u2600-\\u26ff\\u2700-\\u27ff\\u2800-\\u28ff\\u2900-\\u29ff\\u2a00-\\u2aff\\u2b00-\\u2bff\\u2c00-\\u2cff\\u2d00-\\u2dff\\u2e00-\\u2eff\\u2f00-\\u2fff\\u3000-\\u30ff\\u3100-\\u31ff\\u3200-\\u32ff\\u3300-\\u33ff\\u3400-\\u34ff\\u3500-\\u35ff\\u3600-\\u36ff\\u3700-\\u37ff\\u3800-\\u38ff\\u3900-\\u39ff\\u3a00-\\u3aff\\u3b00-\\u3bff\\u3c00-\\u3cff\\u3d00-\\u3dff\\u3e00-\\u3eff\\u3f00-\\u3fff\\u4000-\\u40ff\\u4100-\\u41ff\\u4200-\\u42ff\\u4300-\\u43ff\\u4400-\\u44ff\\u4500-\\u45ff\\u4600-\\u46ff\\u4700-\\u47ff\\u4800-\\u48ff\\u4900-\\u49ff\\u4a00-\\u4aff\\u4b00-\\u4bff\\u4c00-\\u4cff\\u4d00-\\u4dff\\u4e00-\\u4eff\\u4f00-\\u4fff\\u5000-\\u50ff\\u5100-\\u51ff\\u5200-\\u52ff\\u5300-\\u53ff\\u5400-\\u54ff\\u5500-\\u55ff\\u5600-\\u56ff\\u5700-\\u57ff\\u5800-\\u58ff\\u5900-\\u59ff\\u5a00-\\u5aff\\u5b00-\\u5bff\\u5c00-\\u5cff\\u5d00-\\u5dff\\u5e00-\\u5eff\\u5f00-\\u5fff\\u6000-\\u60ff\\u6100-\\u61ff\\u6200-\\u62ff\\u6300-\\u63ff\\u6400-\\u64ff\\u6500-\\u65ff\\u6600-\\u66ff\\u6700-\\u67ff\\u6800-\\u68ff\\u6900-\\u69ff\\u6a00-\\u6aff\\u6b00-\\u6bff\\u6c00-\\u6cff\\u6d00-\\u6dff\\u6e00-\\u6eff\\u6f00-\\u6fff\\u7000-\\u70ff\\u7100-\\u71ff\\u7200-\\u72ff\\u7300-\\u73ff\\u7400-\\u74ff\\u7500-\\u75ff\\u7600-\\u76ff\\u7700-\\u77ff\\u7800-\\u78ff\\u7900-\\u79ff\\u7a00-\\u7aff\\u7b00-\\u7bff\\u7c00-\\u7cff\\u7d00-\\u7dff\\u7e00-\\u7eff\\u7f00-\\u7fff\\u8000-\\u80ff\\u8100-\\u81ff\\u8200-\\u82ff\\u8300-\\u83ff\\u8400-\\u84ff\\u8500-\\u85ff\\u8600-\\u86ff\\u8700-\\u87ff\\u8800-\\u88ff\\u8900-\\u89ff\\u8a00-\\u8aff\\u8b00-\\u8bff\\u8c00-\\u8cff\\u8d00-\\u8dff\\u8e00-\\u8eff\\u8f00-\\u8fff\\u9000-\\u90ff\\u9100-\\u91ff\\u9200-\\u92ff\\u9300-\\u93ff\\u9400-\\u94ff\\u9500-\\u95ff\\u9600-\\u96ff\\u9700-\\u97ff\\u9800-\\u98ff\\u9900-\\u99ff\\u9a00-\\u9aff\\u9b00-\\u9bff\\u9c00-\\u9cff\\u9d00-\\u9dff\\u9e00-\\u9eff\\u9f00-\\u9fff\\ua000-\\ua0ff\\ua100-\\ua1ff\\ua200-\\ua2ff\\ua300-\\ua3ff\\ua400-\\ua4ff\\ua500-\\ua5ff\\ua600-\\ua6ff\\ua700-\\ua7ff\\ua800-\\ua8ff\\ua900-\\ua9ff\\uaa00-\\uaaff\\uab00-\\uabff\\uac00-\\uacff\\uad00-\\uadff\\uae00-\\uaeff\\uaf00-\\uaff\\ub000-\\ub0ff\\ub100-\\ub1ff\\ub200-\\ub2ff\\ub300-\\ub3ff\\ub400-\\ub4ff\\ub500-\\ub5ff\\ub600-\\ub6ff\\ub700-\\ub7ff\\ub800-\\ub8ff\\ub900-\\ub9ff\\uba00-\\ubaff\\ubc00-\\ubcff\\ubd00-\\ubdff\\ube00-\\ubeff\\ubf00-\\ubfff\\uc000-\\uc0ff\\uc100-\\uc1ff\\uc200-\\uc2ff\\uc300-\\uc3ff\\uc400-\\uc4ff\\uc500-\\uc5ff\\uc600-\\uc6ff\\uc700-\\uc7ff\\uc800-\\uc8ff\\uc900-\\uc9ff\\uca00-\\ucaff\\ucb00-\\ucbff\\ucc00-\\uccff\\ucd00-\\ucdff\\uce00-\\uceff\\ucf00-\\ucfff\\ud000-\\ud0ff\\ud100-\\ud1ff\\ud200-\\ud2ff\\ud300-\\ud3ff\\ud400-\\ud4ff\\ud500-\\ud5ff\\ud600-\\ud6ff\\ud700-\\ud7ff\\ud800-\\ud8ff\\ud900-\\ud9ff\\uda00-\\udaff\\udb00-\\udbff\\udc00-\\udcff\\ude00-\\udeff\\udf00-\\udfff\\ue000-\\ue0ff\\ue100-\\ue1ff\\ue200-\\ue2ff\\ue300-\\ue3ff\\ue400-\\ue4ff\\ue500-\\ue5ff\\ue600-\\ue6ff\\ue700-\\ue7ff\\ue800-\\ue8ff\\ue900-\\ue9ff\\uea00-\\ueaff\\ueb00-\\uebff\\uec00-\\uecff\\ued00-\\uedff\\uee00-\\ueeff\\uef00-\\uefff\\uf000-\\uf0ff\\uf100-\\uf1ff\\uf200-\\uf2ff\\uf300-\\uf3ff\\uf400-\\uf4ff\\uf500-\\uf5ff\\uf600-\\uf6ff\\uf700-\\uf7ff\\uf800-\\uf8ff\\uf900-\\uf9ff\\ufa00-\\ufaff\\ufb00-\\ufbff\\ufc00-\\ufcff\\ufd00-\\ufdff\\ufee00-\\ufeff\\ufef00-\\ufeff\\uf000-\\uf0ff\\uf100-\\uf1ff\\uf200-\\uf2ff\\uf300-\\uf3ff\\uf400-\\uf4ff\\uf500-\\uf5ff\\uf600-\\uf6ff\\uf700-\\uf7ff\\uf800-\\uf8ff\\uf900-\\uf9ff\\ufa00-\\ufaff\\ufb00-\\ufbff\\ufc00-\\ufcff\\ufd00-\\ufdff\\ufee00-\\ufeff\\ufef00-\\ufeff\\u2000-\\u20ff\\u2100-\\u21ff\\u2200-\\u22ff\\u2300-\\u23ff\\u2400-\\u24ff\\u2500-\\u25ff\\u2600-\\u26ff\\u2700-\\u27ff\\u2800-\\u28ff\\u2900-\\u29ff\\u2a00-\\u2aff\\u2b00-\\u2bff\\u2c00-\\u2cff\\u2d00-\\u2dff
```



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

amateur

This report was seen 1,027 times.

We are processing your report and will contact the **medialize/uri.js** team with the details of the issue.

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

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[about](#)

[team](#)

[Chat with us](#)