Hostname Spoofing In Urijs

JAVASCRIPT IMPROPER VALIDATION SPOOFING NPM

Yaniv Nizry Feb 13, 2021

Details Overview

Summary

Affected versions of urijs fails to validate the hostname correctly when using backslash in the protocol e.g. `http:\/`. Browsers accept backslashes after the protocol, and treat it as a normal slash, while urijs sees it as a relative path.

Product

urijs before 1.19.6.

Impact

Depending on library usage and attacker intent, impacts may include allow/block list bypasses, SSRF attacks, open redirects, or other undesired behavior.

Steps To Reproduce

```
var URI = require('urijs');
URI('http:/\www.google.com');
```

Expected Result:

the url would be relative without a hostname:

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

Remediation

Update urijs dependency to 1.19.6 or above.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

1. Commit a1ad8bc
2. Release note
3. Advisory