Open Redirect in digitalbazaar/forge

0

✓ Valid Reported on Sep 4th 2021

✍️ Description

`parseUrl` functionality in `node-forge` mishandles certain uses of backslash such as `https:/\/\/\` and interprets the URI as a relative path. Browsers accept backslashes after the protocol, and treat it as a normal slash, while node-forge sees it as a relative path and leads to URL Redirection to Untrusted Site.

🕵️ Proof of Concept

Create the following PoC file:

```
// poc.js
var forge = require("node-forge");
var url = forge.util.parseUrl("https:/\/\/\www.github.com/foo/bar");
console.log(url);
```

Execute the following commands in another terminal:

```
npm i node-forge # Install affected module
node poc.js #  Run the PoC
```

Check the Output:

```
{
  full: 'https://',
  scheme: 'https',
  host: '',
  port: 443,
  path: '/www.github.com/foo/bar',
  fullHost: ''
}
```

```
}
```

In the above example `path` should be `"/foo/bar"` or it should return it as null as per https://github.com/digitalbazaar/forge/blob/c666282c812d6dc18e97b419b152dd6ad98c802c/lib/util.js#L2266

💥 Impact

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

Occurrences

JS util.js L2270

CVE
CVE-2022-0122
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (5.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

ready-research
@ready-research
pro

Chat with us

This report was seen 1,463 times.

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

We have contacted a member of the **digitalbazaar/forge** team and are waiting to hear back a year ago

A **digitalbazaar/forge** maintainer a year ago

Maintainer

The whole `forge.util.parseUrl` API and other URL related APIs were removed in v1.0.0.

ready-research a year ago

Researcher

@maintainer Can you please validate this issue by clicking on `Mark as valid`. And confirm the fix. Thanks.

ready-research modified the report a year ago

A **digitalbazaar/forge** maintainer validated this vulnerability a year ago

ready-research has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **digitalbazaar/forge** maintainer marked this as fixed in **1.0.0** with commit **db8016** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

util.js#L2270 has been validated ✓

> Sign in to join this conversation

Chat with us