Regular Expression Denial of Service (ReDoS) in moment/moment

2

Valid Reported on Jun 6th 2022

Description

Affected versions of the package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks for any string input controlled by the user.
An attacker can provide a specially crafted input to the default function `moment()`, which nearly matches the pattern being matched. This will cause the regular expression matching to take a long time, all the while occupying the event loop and preventing it from processing other requests and making the server unavailable (a Denial of Service attack).

Proof of Concept

```
// PoC.js
moment=require('moment')
moment("(".repeat(50000)) // local execution time ~=0m1.6s
moment("(".repeat(500000)) // local execution time ~=8m49.741s
```

Expected behavior

Execution time has to be linear, not polynomial.

Impact

Any dependent pass user-controllable string inputs to package moment() could cause the denial of service attack. It happens in the default use of the package and potentially affects around 57,775 dependents *(last access: June 7 2022)*.

Occurrences

JS from-string.js L154

CVE

CVE-2022-31129
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
High (7.5)

Registry
Npm

Affected Version
All version

Visibility
Public

Status
Fixed

Found by

Khang Vo (doublevkay)

@vovikhangcdv

master

Fixed by

Khang Vo (doublevkay)

@vovikhangcdv

master

This report was seen 1,941 times.

We are processing your report and will contact the **moment** team within 24 hours. 6 months ago

Khang Vo (doublevkay) modified the report 6 months ago

Khang Vo (doublevkay) submitted a patch 6 months ago

Khang Vo (doublevkay) modified the report 6 months ago

Khang Vo (doublevkay) modified the report 6 months ago

We created a GitHub Issue asking the maintainers to create a `SECURITY.md` 6 months ago

Iskren Ivov Chernev validated this vulnerability 5 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

Khang 5 months ago Researcher

Hey @Iskren (@maintainer),
The fixed version has already been released. Could we fully disclose this report too?

Iskren Ivov Chernev marked this as fixed in 2.24.4 with commit 9a3b58 5 months ago

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

This vulnerability will not receive a CVE ❌

from-string.js#L154 has been validated ✅

Khang 5 months ago Researcher

Hi @admin, the vulnerability has been assigned CVE-31129. Could you help to change the CVE ID status of this report?

Jamie Slome 5 months ago Admin

Sorted 👍

Sign in to join this conversation

Chat with us