

New issue

Jump to bottom

ArrayIndexOutOfBoundsException in parser #67

Closed

pcy190 opened this issue on Apr 15, 2021 · 7 comments

Assignees



Labels

bug

pcy190 commented on Apr 15, 2021 • edited

Contributor

Same as
netplex/json-smart-v1#10

The code base is at

```
json-smart-v2/json-smart/src/main/java/net/minidev/json/parser/JSONParserByteArray.java
Lines 77 to 82 in 00955f7
77     protected int indexOf(char c, int pos) {
78         for (int i = pos; pos < len; i++)
79             if (in[i] == (byte) c)
80                 return i;
81         return -1;
82     }
```

It shouldn't be the pos to be checked less than len. Instead, the i should be checked. The correct way in line 79 is:

```
for (int i = pos; i < len; i++)
```

Any input with unclosed single quotation mark could trigger this. Like the input of 'c, cause the ArrayIndexOutOfBoundsException

pcy190 mentioned this issue on Apr 15, 2021

Fix ArrayIndexOutOfBoundsException #68

Merged

UrielCh added the bug label on Apr 17, 2021

UrielCh assigned pcy190 on Apr 17, 2021

UrielCh commented on Apr 23, 2021

Contributor

Hi,

I did not see any Deny of Service factor, in this project. If this bug is used, it will just reject the JSON with an incorrect error message.

If you really see a DOS attack here, provide me a proof of concept.

1

UrielCh commented on Apr 23, 2021

Contributor

Upgrading the json-smart version now, may not be the proper time due to #69, a pom file may still be missing from the maven repo. I think the issue is solved but I did not get any confirmation of that.

So I prefer to wait 24 hours, and the release of the V2.5.0.

If you want to create a new CVE-2021-XXXXXX vulnerability alert do so.

UrielCh commented on May 2, 2021

Contributor

As I told you, for me, it's not a security issue, and this bug can not cause a DOS attack.

by the way, it is fixed in 3 branches

- V1.3.X
- V 2.3.X
- V2.4.X

UrielCh closed this as completed on May 2, 2021

codefish1 commented on Jun 14, 2021


@UrielCh this hasn't been applied to the 2.3 branch <https://github.com/netplex/json-smart-v2/blob/v2.3/json-smart/src/main/java/net/minidev/json/parser/JSONParserByteArray.java> is it possible to get it applied and a new release made?

UrielCh commented on Jun 15, 2021

Contributor

upgrading to 2.4 is not enough?

I'm waiting for more feedback before making a new release.

 UrielCh reopened this on Jun 15, 2021

pcy190 commented on Jun 15, 2021

Contributor Author

Note that this is tied to [CVE-2021-31684](#)

codefish1 commented on Jun 15, 2021 • edited

I'm using it via spring boot 2.4 who have upgraded to 2.3.1 but my employer still blocks the new 2.3.1 release due to [CVE-2021-31684](#). I've personally excluded and re-added but I believe spring boot will automatically update to a 2.3.2 release with their next patch and then this will be fixed for others as well.

 pcy190 closed this as completed on Jun 19, 2021

 This was referenced on Jun 24, 2021

!!!URGENT!!! Upgrading to json-smart 2.4.5 causes missing dependency net.minidev:accessors-smart:jar:2.4.3 netplex/json-smart-v1#14

 Open

!!!URGENT!!! Upgrading to json-smart 2.4.5 causes missing dependency net.minidev:accessors-smart:jar:2.4.3 #76

 Closed

 This was referenced on Jun 1

Suppress CVEs apache/druid#12590

 Merged

Suppress CVEs (#12590) - Backport to 0.23.0 apache/druid#12597

 Merged

Assignees

 pcy190

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants