New issue

Jump to bottom

Uncaught Exception in Parser #7

Closed GanbaruTobi opened this issue on Feb 22, 2021 · 2 comments

GanbaruTobi commented on Feb 22, 2021 • edited

The parser fails to throw the ParseException when the parser expects the input to be of the float number type AND the input not being a valid number. This can lead to uncaught exceptions by unexpected input, which may lead to Denial-of-Service (DoS).

json-smart-v1/json-smart/src/main/java/net/minidev/json/parser/JSONParserBase.java
Lines 134 to 142 in 51e1641

```
134     protected Number extractFloat() throws ParseException {
135             if (!acceptLeadinZero)
136                     checkLeadinZero();
137             if (!useHiPrecisionFloat)
138                     return Float.parseFloat(xs);
139             if (xs.length() > 18) // follow JSonIJ parsing method
140                     return new BigDecimal(xs);
141             return Double.parseDouble(xs);
142     }
```

Parser Input of "-." or "2e+" or "[45e-" will crash with a NumberFormatException.

```
== Java Exception: java.lang.NumberFormatException: For input string: "-."
        at java.base/jdk.internal.math.FloatingDecimal.readJavaFormatString(FloatingDecimal.java:2054)
        at java.base/jdk.internal.math.FloatingDecimal.parseDouble(FloatingDecimal.java:110)
        at java.base/java.lang.Double.parseDouble(Double.java:549)
        at net.minidev.json.parser.JSONParserBase.extractFloat(JSONParserBase.java:141)
        at net.minidev.json.parser.JSONParserMemory.readNumber(JSONParserMemory.java:81)
        at net.minidev.json.parser.JSONParserBase.readMain(JSONParserBase.java:379)
        at net.minidev.json.parser.JSONParserBase.parse(JSONParserBase.java:156)
        at net.minidev.json.parser.JSONParserString.parse(JSONParserString.java:56)
        at net.minidev.json.parser.JSONParserString.parse(JSONParserString.java:37)
        at net.minidev.json.parser.JSONParser.parse(JSONParser.java:140)
```

👍 1

This was referenced on Feb 23, 2021

Findings CodeIntelligenceTesting/jazzer#19
Closed

Uncaught Exception in Parser - Possible Fix #8
Merged

pronovic commented on Mar 12, 2021

Note that this is tied to CVE-2021-27568, categorized as base score 9.1 (critical).

oscerd mentioned this issue on Mar 23, 2021

Moving away from Json-smart tomj74/chunk-templates#37
Closed

UrielCh commented on Apr 4, 2021 Contributor

New version released 1.3.2 with CVE-2021-27568 fixed
json-smart-mini had also been patched and released.

UrielCh closed this as completed on Apr 4, 2021

This was referenced on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar - autoclosed rsoreq/zaproxy#112
Closed

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar billmcchesney1/foxtrot#298
Open

CVE-2021-27568 (High) detected in json-smart-2.3.jar RG4421/spark-tpcds-benchmark#30
Open

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar LevyForchh/karate#138
Open

CVE-2021-27568 (High) detected in json-smart-2.3.jar, json-smart-2.2.1.jar jmacwhitesource/cloud-pipeline#354

Open

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar Mohib-hub/karate#135

Open

CVE-2021-27568 (High) detected in json-smart-2.3.jar keanhankins/ranger#224

Open

mend-bolt-for-github bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar heltondoria/DemoApplication#162

Open

mend-for-github-com bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar rammatzkvosky/cwa-server#27

Open

This was referenced on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar - autoclosed liorzilberg/swagger-parser#536

Closed

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar gsylvie/t#193

Open

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar safat/conductor#176

Open

mend-for-github-com bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar rammatzkvosky/nakadi#105

Open

mend-bolt-for-github bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar hiucimon/ClamScanService#103

Open

mend-for-github-com bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-1.2.jar, json-smart-2.3.jar SmartBear/readyapi4j#199

Open

mend-bolt-for-github bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar greenetx/jenkins2-course-spring-boot#241

Open

This was referenced on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar - autoclosed swagger-api/swagger-core#3920

Closed

CVE-2021-27568 (High) detected in json-smart-2.3.jar mwilliams7197/calcite-kudu#9

Open

mend-bolt-for-github bot mentioned this issue on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.2.1.jar nicholaswkc34/Spring_Rest#104

Open

This was referenced on Apr 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.1.1.jar - autoclosed SmartBear/readyapi-swagger-assertion-plugin#138

Closed

CVE-2021-27568 (High) detected in json-smart-2.3.jar - autoclosed SmartBear/ready-mqtt-plugin#135

Closed

CVE-2021-27568 (High) detected in json-smart-1.2.jar - autoclosed SmartBear/soapui#606

Closed

CVE-2021-27568 (High) detected in json-smart-2.3.jar - autoclosed SmartBear/ready-jira-plugin#162

Closed

CVE-2021-27568 (High) detected in json-smart-1.2.jar - autoclosed SmartBear/ready-aws-plugin#150

Closed

71 hidden items
Load more...

This was referenced on Nov 6, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar samqws-marketing/box_mojito#94
Open

CVE-2021-27568 (High) detected in json-smart-2.3.jar Dima2022/concord-plugins#28
Open

This was referenced on Dec 7, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar harrinry/spring-cloud-config#41
Open

CVE-2021-27568 (High) detected in json-smart-2.3.jar Snootch17/jdbc#13
Open

mend-bolt-for-github bot mentioned this issue on Dec 13, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar txh51591/tm-repo#83
Open

mend-for-github-com bot mentioned this issue on Dec 17, 2021

CVE-2021-27568 (High) detected in json-smart-2.3.jar samjcs/snowflake-jdbc#4
Open
1 task

mend-for-github-com bot mentioned this issue on Jan 6

CVE-2021-27568 (High) detected in json-smart-2.3.jar dmyers87/camunda-message-streaming#30
Open

mend-for-github-com bot mentioned this issue on Jan 13

CVE-2021-27568 (High) detected in json-smart-2.3.jar harrinry/DataflowTemplates#31
Open

mend-bolt-for-github bot mentioned this issue on Feb 7

CVE-2021-27568 (High) detected in json-smart-2.3.jar hapifhir/hapi-fhir#3362
Open

This was referenced on Feb 7

CVE-2021-27568 (High) detected in json-smart-2.3.jar swagger-api/swagger-codegen#11702
Open

spring-boot-starter-test-2.5.5.jar: 1 vulnerabilities (highest severity is: 9.1) joshnewton31080/graphql-kotlin#10
Open

mend-bolt-for-github bot mentioned this issue on Mar 7

CVE-2021-27568 (High) detected in json-smart-2.3.jar - autoclosed mgh3326/que_bang#90
Closed

This was referenced on Mar 23

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#15
Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#21
Open

This was referenced on Mar 31

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#26
Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#31
Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#36

Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#41

Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#46

Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#51

Open

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#56

Open

This was referenced on Apr 13

nimbus-jose-jwt-8.3.jar: 1 vulnerabilities (highest severity is: 9.1) rjg-ws-demo/SasanLabs-VulnerableApp#61

Open

spring-boot-starter-test-2.1.4.RELEASE.jar: 1 vulnerabilities (highest severity is: 9.1) timf-app-sandbox/terracotta-bank#17

Open

spring-boot-starter-test-1.5.1.RELEASE.jar: 3 vulnerabilities (highest severity is: 9.1) timf-app-sandbox/terracotta-bank#20

Open

This was referenced on Jun 2

spring-boot-starter-test-2.4.5.jar: 4 vulnerabilities (highest severity is: 9.1) Nexmo/java-skeleton-app#2

Open

spring-boot-starter-test-2.4.5.jar: 4 vulnerabilities (highest severity is: 9.1) Nexmo/vonage-spring-boot-starter-java#10

Open

wiremock-1.58.jar: 8 vulnerabilities (highest severity is: 9.1) opentok/Opentok-Java-SDK#221

Open

This was referenced 3 days ago

json-smart-2.3.jar: 1 vulnerabilities (highest severity is: 9.1) mojombo/god#279

Open

lwc-functional-test-1.6.jar: 1 vulnerabilities (highest severity is: 9.1) mojombo/god#308

Open

lwc-core-2.0.3.jar: 27 vulnerabilities (highest severity is: 9.8) mojombo/god#363

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants