



CVE-2023-4043

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-4043
State	PUBLIC
Assigner	security@eclipse.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 09:15:00 UTC
Updated	2023-11-13 18:26:00 UTC
Description	In Eclipse Parsson before versions 1.1.4 and 1.0.5, Parsing JSON from untrusted sources can lead malicious actors to exploit

Risk And Classification

Problem Types: CWE-834

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Parsson	All	All	All	All

References

Reference

- BigInteger scale limit counts absolute value now. by Tomas-Kraus · Pull Request #100 · eclipse-ee4j/parsson · GitHub
- There is a DoS vulnerability in the latest version 2.1.2 of jakartaee/jsonp-api (#13) · Issues · Eclipse Projects Security / vulnerability-reports · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 20401 Oracle Database 21c Critical Patch Update - January 2024
- 243042 Red Hat Update for JBoss Enterprise Application Platform 8.0.1 (RHSA-2024:1193)
- 243044 Red Hat Update for JBoss Enterprise Application Platform 8.0.1 (RHSA-2024:1192)
- 995833 Java (Maven) Security Update for org.eclipse.parsson:project (GHSA-g8p6-p27c-52fx)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)