(https://github.com/eclipse/rdf4j)

(https://rdf4j.org/)™

5.3.2

RDF4J 5.3.2 is a patch release that fixes 2 issues, including a security fix for XML parsing.

For a complete overview, see all issues fixed in 5.3.2 (https://github.com/eclipse/rdf4j/milestone/130?closed=1).

Security

This release fixes XML parsing paths that were not fully covered by the earlier fix for CVE-2018-1000644 (https://nvd.nist.gov/vuln/detail/CVE-2018-1000644). The vulnerability class is XML External Entity (XXE) processing: specially crafted XML input may attempt to make the parser resolve external entities or DTDs, with risks such as confidential data disclosure, denial of service, or server-side requests.

RDF4J 5.3.2 closes related gaps in RDF4J's XML parser setup, including paths used for RDF/XML, TriX, SPARQL/XML results, DOM helper parsing, transaction XML parsing, and server-boot `web.xml` parsing. XML parser defaults are now hardened consistently so DOCTYPE declarations, external entities, and external DTD loading are rejected or disabled by default.

Users who parse untrusted XML-based RDF4J data or query results are strongly encouraged to upgrade.

Acknowledgements

This release was made possible by contributions from Kairo de Araujo.

Table of Contents

Back to the top