

Vulnerability Report Document

BOM Format: CycloneDX

Specification Version: 1.4

Version: 1

Vulnerabilities

1. ID: **CVE-2020-25649**

Description: com.fasterxml.jackson.core:jackson-databind is a library which contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor.

Affected versions of this package are vulnerable to XML External Entity (XXE) Injection. A flaw was found in FasterXML Jackson Databind, where it does not have entity expansion secured properly in the DOMDeserializer class. The highest threat from this vulnerability is data integrity.

- **Severity:** high (CVSSv31 — Source: NVD)
- **Severity:** high (CVSSv31 — Source: SNYK)
- **Severity:** none (CVSSv31 — Source: Acme Inc)

Analysis: Not Affected

- **Justification:** Code Not Reachable
- **Details:** Automated dataflow analysis and manual code review indicates that the vulnerable code is not reachable, either directly or indirectly.