

Welcome to Sonatype Nexus Lifecycle.



# Vulnerability Lookup

## Find Results on Specific Vulnerabilities

All vulnerability lookups must use an exact match to surface a result.

Find

### sonatype-2018-0624

#### Issue

sonatype-2018-0624

#### Severity

Sonatype CVSS 3: 9.8

CVE CVSS 2.0: 0.0

#### Weakness

Sonatype CWE: 611 [↗](https://cwe.mitre.org/data/definitions/611.html)  
(<https://cwe.mitre.org/data/definitions/611.html>)

#### Source

Sonatype Data Research

#### Categories

Data

#### Explanation

The `woodstox-core` package is vulnerable to Improper Restriction of XML eXternal Entity (XXE) Reference. The `setFeature` and `getFeature` methods in `WstxSAXParserFactory.class` rely on the `mSecureProcessing` boolean value to be able to securely parse input XML. The boolean value, however, is set to `false` by default. Additionally, the class lacks support for properties `XMLConstants.FEATURE_SECURE_PROCESSING` and `XMLInputFactory.IS_SUPPORTING_EXTERNAL_ENTITIES`, which can make it possible for an attacker to conduct XXE attacks.

#### Detection

The application is vulnerable by using this component.

#### Advisories

- Project: <https://github.com/FasterXML/woodstox/issues/50> [↗](#) (<https://github.com/...>)
- Project: <https://github.com/FasterXML/woodstox/issues/51> [↗](#) (<https://github.com/...>)
- Project: <https://github.com/FasterXML/woodstox/issues/61> [↗](#) (<https://github.com/...>)

#### CVSS Details

Sonatype CVSS 3: 9.8

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H