Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Apache Calcite 1.22.0 introduced the SQL operators EXISTS_NODE, EXTRACT_XML, XML_TRANSFORM and EXTRACT_VALUE do not restrict XML External Entity references in their configuration, making them vulnerable to a potential XML External Entity (XXE) attack.

Technical Details

Any client exposing these operators, typically by using Oracle dialect (the first three) or MySQL dialect (the last one), is affected by this vulnerability (the extent of it will depend on the user under which the application is running). From Apache Calcite 1.32.0 onwards, Document Type Declarations and XML External Entity resolution are disabled on the impacted operators.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2022-39135
- https://lists.apache.org/thread/ohdnhlgm6jvt3srw8l7spkm2d5vwm082
- http://www.openwall.com/lists/oss-security/2022/11/21/3