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 an attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize javax.script.ScriptEngineManager to load code using that ClassLoader. Affects all the versions 1.2.0 or lower.

Technical Details

This unbounded deserialization can likely lead to remote code execution. The code can be run in Helix REST start and Workflow creation.

Short term Mitigation: stop using any YAML based configuration and workflow creation.

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-2023-38647
- https://lists.apache.org/thread/zyqxhv0lc2z9w3tgr8ttrdy2zfh5jvc4
- https://helix.apache.org/