Overall Rating - Critical

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a Java object deserialization issue in Jackrabbit webapp/standalone on all platforms allows attacker to remotely execute code via RMIVersions up to (including) 2.20.10 (stable branch) and 2.21.17 (unstable branch) use the component "commons-beanutils", which contains a class that can be used for remote code execution over RMI.

Technical Details

RMI support can expose vulnerabilities by the mere presence of an exploitable class on the classpath. Even if Jackrabbit itself does not contain any code known to be exploitable anymore, adding other components to your server can expose the same type of problem.

How to check whether RMI support is enabledRMI support can be over an RMI-specific TCP port, and over an HTTP binding. Both are by default enabled in Jackrabbit webapp/standalone. The native RMI protocol by default uses port 1099. To check whether it is enabled, tools like "netstat" can be used to check. RMI-over-HTTP in Jackrabbit by default uses the path "/rmi". So, when running standalone on port 8080, check whether an HTTP GET request on localhost:8080/rmi returns 404 (not enabled) or 200 (enabled). Note that the HTTP path may be different when the webapp is deployed in a container as non-root context, in which case the prefix is under the user's control. Turning off RMIFind web.xml (either in JAR/WAR file or in unpacked web application folder), and remove the declaration and the mapping definition for the RemoteBindingServlet: <servlet> <servlet-name>RMI</servlet-name> <servlet-class>org.apache.jackrabbit.servlet.remote.RemoteBindingServlet</servlet-class> </servlet> <servlet-mapping> <servlet-name>RMI</servlet-name> <url-pattern>/rmi</url-pattern> </servlet-mapping> Find the bootstrap.properties file (in $REPOSITORY_HOME), and set rmi.enabled=false and also remove rmi.host rmi.port rmi.url-pattern If there is no file named bootstrap.properties in $REPOSITORY_HOME, it is located somewhere in the classpath. In this case, place a copy in $REPOSITORY_HOME and modify it as explained.

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-2023-37895

https://lists.apache.org/list.html?users@jackrabbit.apache.org
https://jackrabbit.apache.org/