Dependabot

The ASF Infra team has approved and enabled Dependabot on the ASF Github repositories.

In Sling we have long had a policy of depending on the lowest possible version of the API, to ensure that our bundles are deployed in the widest possible ra nge of environments. Therefore the responsibility of ensuring that the environment is secure lies with the assembler and/or deployer of the application, which should make sure that the OSGi bundles they deploy are secure.

Therefore, we will reject pull requests that update dependencies of OSGi bundles.

As an exception, pull requests targeting the following are useful and should be merged:

- libraries that are embedded/inlined in OSGi bundles since those will end up deployed directly
- dependencies of Maven plug-ins
- bundles that are deployed directly in applications like the Sling Starter, the Sling Karaf Features, or the Sling CMS
- dependencies of projects written in Node.js

It is possible to configure dependabot directly using the .asf.yaml file, see Git - .asf.yaml features#DependabotAlertsandUpdates .