8
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7525
com.fasterxml.jackson.core : jackson-databind : 2.8.6 jackson-databind-2.8.6.jar

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15095
com.fasterxml.jackson.core : jackson-databind : 2.8.6 jackson-databind-2.8.6.jar

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7525
org.codehaus.jackson : jackson-mapper-asl : 1.9.13 jackson-mapper-asl-1.9.13.jar

These are all related to https://jira.magnolia-cms.com/browse/MAGNOLIA-7313.

According to jackson-databind: the fix of (CVE-2017-7525) is introduced from 2.8.9 . See https://github.com/FasterXML/jackson-databind/issues/1599.

Note: There are some updates from jackson related to other CVE issues: https://github.com/FasterXML/jackson-databind/issues?utf8=%E2%9C%93&q=label%3ACVE+.

Action taken:
Magnolia will use RESTEasy shipped with newer jackson-databind versions by updating RESTEasy to 3.5.1.Final.

A PR has already been made against Magnolia 5.7, which is expected to ship 15 June.

7
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4002
xerces : xercesImpl : 2.8.1 xercesImpl-2.8.1.jar

This is related to Java versions (Java Runtime Environment (JRE) in IBM Java 5.0 before 5.0 SR16-FP3, 6 before 6 SR14, 6.0.1 before 6.0.1 SR6, and 7 before 7 SR5)

Action taken:
None necessary. Magnolia 5.x+ is based on Java 8. Java 9 and 10 support is being worked into future versions. As can be seen here: https://documentation.magnolia-cms.com/display/DOCS56/Certified+stack, current versions of Magnolia do not support the affected Java versions.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5651
org.apache.tomcat : tomcat-coyote : 8.5.5 tomcat-coyote.jar

This is related to Tomcat versions. Tomcat is a container on which Magnolia may be deployed.

Action taken:
None necessary. It is up to the entity deploying Magnolia to make sure Magnolia is deployed on the appropriate containers and versions. The current certified stack may be found here: https://documentation.magnolia-cms.com/display/DOCS56/Certified+stack.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3253
org.codehaus.groovy : groovy-all : 2.4.3 groovy-all-2.4.3.jar

Magnolia currently uses version 2.3.4 of this library, which is technically affected.

Action taken:
Magnolia 6.0 will use the latest version of this library (2.4.5), according to MGNLGROOVY-167. Magnolia 6.0 is expected to ship 15 November. A patch can be made in the interim.

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0114
commons-beanutils : commons-beanutils : 1.9.3 commons-beanutils-1.9.3.jar

This is related to Magnolia's bean-resolving mechanism.

Action taken:
The latest version of Magnolia uses version 1.9.3 of this library. The vulnerability states that version up to 1.9.2 are affected (it is fixed in 1.9.2 with

***https://commons.apache.org/proper/commons-beanutils/javadocs/v1.9.3/RELEASE-NOTES.txt* - see BEANUTILS-463). Therefore, Magnolia is not affected by this vulnerability.**

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0254
javax.servlet : jstl : 1.2 jstl-1.2.jar

This is related to apache standard-taglibs, which are not used by Magnolia. Therefore this vulnerability does not affect Magnolia.

Action taken:
None necessary.