

Issues	Library	Related Link	Comment	Note
Improper Certificate Validation in xmlHttpRequest-ssl	xmlHttpRequest-ssl	https://github.com/advisories/GHSA-72mh-269x-7mh5	There is no direct dependency so Nuxeo doesn't hold any responsibility for managing this library	
xmlHttpRequest and xmlHttpRequest-ssl vulnerable to Arbitrary Code Injection	xmlHttpRequest-ssl	https://github.com/advisories/GHSA-h4j5-c7cj-74xg	There is no direct dependency so Nuxeo doesn't hold any responsibility for managing this library	
Misinterpretation of malicious XML input	xmldom	https://github.com/advisories/GHSA-5fg8-2547-mr8q	The current version is enough to support XXe attack protection	
Arbitrary Code Execution in underscore	underscore	https://github.com/advisories/GHSA-cf4h-3jhx-xvhq	No direct dependency	
thenify before 3.3.1 made use of unsafe calls to `eval`.	thenify	https://github.com/advisories/GHSA-29xr-v42j-r956	No direct dependency	
Resource exhaustion in socket.io-parser	socket.io-parser	https://github.com/advisories/GHSA-xfhh-g9f5-x4m4	Will auto manage by wdio upgrade	
Insufficient validation when decoding a Socket.IO packet	socket.io-parser	https://github.com/advisories/GHSA-qm95-pgcb-qcfc	Will auto manage by wdio upgrade	
Prototype pollution in Plist before 3.0.5 can cause denial of service	plist	https://github.com/advisories/GHSA-4cpg-3vgw-4877	No direct dependency	
Prototype Pollution in minimist	minimist	https://github.com/advisories/GHSA-vh95-rmgr-6w4m	It's a security issue we have to look for a solution	This has not affected directly the project and we found some warnings while updating the node js, we can take care of this after the Nodejs update
Prototype Pollution in lodash	lodash.template	https://github.com/advisories/GHSA-jf85-cpcp-j695	current version is enough for now we will upgrade this later	
Regular Expression Denial of Service (ReDoS) in lodash	lodash	https://github.com/advisories/GHSA-x5rg-j2xg-h7qm	current version is enough for now we will upgrade this later	
Command injection in launchpad	launchpad	https://github.com/advisories/GHSA-7h8x-wmq2-7mff		
json-schema is vulnerable to Prototype Pollution	json-schema	https://github.com/advisories/GHSA-896r-f27r-55mw	try to update to latest compatible version	This is a peer dependency, this does not directly impact the NodeJs upgrade we can take care of this after the NodeJs update.
Arbitrary Code Execution in handlebars	handlebars	https://github.com/advisories/GHSA-q2c6-c6pm-g3gh	No direct dependency	
Malware in fsevents	Severity	https://github.com/advisories/GHSA-xv2f-5jw4-v95m	NA (No threat)	
ejs template injection vulnerability	Severity	https://github.com/advisories/GHSA-phwq-i96m-2c2q	NA (No threat)	
Prototype Pollution in deep-extend	Severity	https://github.com/advisories/GHSA-hr2v-3952-633q	NA (No threat)	