Dependency Analysis

Module	Description	version	Dep chain	Top?	Make an issue?	SEC
tesla (npm,gh)	MVC Style Framework for Node.js	0.5.0	superagent(~0.18)->qs(0.6.6)	Depends		
jsreport (npm, gh)	**Open source platform for designing and rendering various reports.**	**0.1.14**	jaydata(*)->qs(0.5.0)	Depends		
radiatus (npm, gh)	Radiatus is a web server for freedom.js applications, built using node.js, express, and freedom-for-node.	0.0.2	body-parser(~1.5.2)->qs(0.6.6)	Depends	gh uses body-parser(`~1.12.0`)	
tarifa(npm, gh)	tarifa is a CLI on top of Apache Cordova. It aims at	0.2.5	restler(3.2.2)->qs(0.6.6)	Depends	latest version of restler -> no option	

	simplifying the Apache Cordova workflow and adding features to complete cordova toolchain					
ionic(npm, gh)	The Ionic Framework command line utility makes it easy to start, build, run, and emulate Ionic apps. In the future, it will also have support for our mobile development services and tools that make Ionic even more powerful.	1.2.8-beta1	tiny-lr-fork(0.0.5)->qs(~0.5.2)	downloads		
juice(npm, gh)	Given HTML, juice will inline your	0.5.0	superagent(0.18.2)->qs(0.6.6)	downloads ,stars	resolved	yes, solved

	CSS properties into the `style` attribute.					
component(npm, gh)	Component is a vertically integrated frontend solution, handling everything from package management to the build process, handling everything including HTML, JS, CSS, images, and fonts. Think of it as an opinionated `npm + browserify + rework-npm + grunt/gulp/broccoli` all wrapped into`component build`.	1.0.0-rc7	tiny-lr-fork(0.0.5)->qs(~0.5.2) superagent!!!	downloads		
feedparser (npm,gh)	Robust RSS,	0.19.2	resanitize(~0.3.0)<-validator(~1.5.1)	downloads ,stars	Yes, but on resanitize,	No

	Atom, and RDF feed parsing in Node.js				not in a vulnerable state	
juice2(npm, gh)	Juice inlines CSS stylesheets into your HTML source.	1.3.0	superagent(~0.18.2)->qs(0.6.6)	downloads		
ripple-lib(npm, gh)	A JavaScript API for interacting with Ripple in Node.js and the browser	0.9.0-rc2	superagent(^0.18.0)->qs(0.6.6)	downloads,stars		
harp(npm, gh)	Static Site Server/Generator with built-in preprocessing http://harpjs.com	0.14.0	terraform(0.9.0)<-marked(0.2.9)	downloads,stars		Yes, solved
atomify(npm, gh)	Atomic web development - Combining the power of npm, Browserify, Rework	5.0.0	• tiny-lr-fork(0.0.5)->qs(~0.5.2) • atomify-css(^3.0.0)<-npm-less(^1.0.0)<-request(~2.39.0)<-qs(~0.6.0)	downloads,stars		Yes, updated

	and more to build small, fully encapsulated client side modules					
loopback-component-storage(npm, gh)	LoopBack storage component provides Node.js and REST APIs to manage binary contents using pluggable storage providers, such as local file systems, Amazon S3, or Rackspace cloud files	1.0.5	pkgcloud(~0.9.6)<-qs(0.6.x)	downloads	resolved	
shout(npm, gh)	The self-hosted web IRC client http://shout-irc.com/	0.44.0	superagent(^0.18.2)->qs(0.6.6)	downloads,stars	resolved	Yes, but not NSP
roots(npm, gh)	a toolkit for rapid	3.0.0-rc.10	charge(0.0.3)<-pathologist-middleware (0.0.1)<-send(^0.3.0	downloads,stars		

	advanced front-end development http://roots.cx		)			
open.core(npm,gh)	Common utility functionality used between multiple applications.	0.1.209	restler(>=0.2.1)<-qs(0.6.6)	downloads		
quips(npm,gh)	a leak-plugging layer on top of backbone.js	1.0.20	hem-haml-coffee(0.0.3)<-hem(*)<-connect(~2.6.0)	downloads		
yogi(npm,gh)	Command Line Helper for YUI http://yui.github.com/yogi/	0.1.13	yuidocjs(~0.3.31)<-marked(~0.2.8)	downloads		Yes, production tool!
sear(npm,gh)	SEAR: To brown very quickly by intense heat. This method increases shrinkage but develops	0.0.24	brucedown(~0.1.1)<-marked(~0.2.5)	downloads		

	flavor and improves appearance. Bake(r) was taken.					
sendwithus(npm,gh)	Send With Us node client	2.5.0	restler(~3.2.2)<-qs(0.6.6)	downloads		
taskcluster-base(npm,gh)	A collection of common modules used many taskcluster components. Most of the modules in this *base* collection can be instantiated by	0.6.0	superagent(0.18.2)->qs(0.6.6)	downloads		

	providing a JSON dictionary with configuration and parameters.					
manta(npm,gh)	Node.js SDK for Manta	1.4.5	restify(2.8.1)->qs(0.6.6)	downloads	intressant!	
fekit(npm, gh)	FE Toolkit	0.2.80	connect(2.7.x)	forks		
gitbook(npm, gh)	Modern book format and toolchain using Git and Markdown https://www.gitbook.com	1.10	send(0.2.0)	stars		Yes
socketstream(npm, gh)	A framework for Realtime Web Apps http://socketstream.com	0.3.10	connect(=2.4.5)	stars	diff version on gh, but solved	Yes, but not NSP

everyauth-goellan(npm,gh)	Node.js auth package (password, facebook, & more) for Connect and Express apps http://everyauth.com/	0.2.32	connect(>=1 <2)	stars	solved	Yes, solved
plupload(npm, gh)	Plupload is a JavaScript API for dealing with file uploads it supports features like multiple file selection, file type filtering, request chunking, client side image scaling and it uses different runtimes to achieve this such as HTML	2.1.2	yuidocjs(0.3.x)<-marked(~0.2.8)	stars		

	5, Silverlight and Flash					
batman.js(npm, gh)	The best JavaScript framework for Rails developers. http://batmanjs.org	0.15.0	connect(~2.7.4)	stars		
phpjs(npm, gh)	php.js implements PHP functions in JavaScript http://phpjs.org	1.3.2	send(0.1.0)	stars	gh updated, but npm not	
cleaver(npm, gh)	30-second slideshows for hackers	0.7.2	marked(~0.2.9)	stars		
calipso(npm, gh)	Calipso is a simple NodeJS content management system based on Express, Connect & Mongoose.	0.3.50	connect(2.3.x) **qs** 0.4.x	stars		Yes, but not NSP

restler(npm, gh)	REST client library for node.js	3.2.2	qs(0.6.6)	stars	gh updated, but not npm!! action: update the npm, then problem is solved!!	Yes

pump.io(npm, gh)	Social server with an ActivityStreams API http://pump.io/	0.3.0	connect(1.x)
			validator(0.4.x)
				stars	Yes!	Yes, on website and some issues

styledocco (npm,gh)	Automatically generate a style guide from your stylesheets. http://jacobrask.github.com/styledocco/	0.6.6	marked(0.2.x)	stars		
connect-auth(npm, gh)	Authentication middleware for connect.	0.6.1	connect(2.7.x)	stars		Yes, but no action taken
locomotive (npm,gh)	Powerful MVC web framework for Node.js	0.4.2	syntax-error(0.0.1)	stars		Yes, reported but no action

handlebars-helpers(npm, gh)	Library of 120+ handlebars helpers for any project: Assemble, Ghost, YUI... This project is active and supported, we love contributors and appreciate stars. http://assemble.io/helpers/	0.5.8	marked(~0.2.10)	stars		Yes, had some breaking changes
matador(npm, gh)	an MVC framework for Node http://medium.github.io/matador	2.0.0-alpha.5	connect(2.3.3)	stars	make an issues!!!!!	
yuidocjs (npm, gh)	YUI Javascript Documentation Tool http://yui.github.com/yuidoc	0.3.50	marked(~0.2.8)	stars	resolved	Yes
papery (npm, gh)	Papery - Create your	0.2.4-2	marked-toc(^0.2.6)<-marked(0.3.0)	stars		

	simple, fast & elegant blog with plain text					
hem(npm, gh)	Bundler for Node/CommonJS/Web Apps	0.3.6	connect(~2.6.0)	stars		
rrestjs(npm, gh)	High performance nodejs framework http://rrest.cnodejs.net	1.3.5	qs(0.5.1)	stars		
express-admin (npm, gh)	MySQL, MariaDB, SQLite, PostgreSQL admin for NodeJS	1.2.5	connect-multiparty(1.1.0)<-qs(~0.6.5)	stars		
hippie(npm,gh)	End-to-end API testing made easy	0.3.0	qs(~0.6.5)	stars		
mailchimp(npm,gh)	A node.js wrapper for the MailChimp API.	1.1.0	qs(0.5.x)	stars		
shiny-server(npm,gh)	Host Shiny applicatio	0.3.6	send(0.1.x)	stars		

	ns over the web. http://rstudio.com/shiny/server					
imager (npm,gh)	A node.js module to resize, crop and upload images to Rackspace cloudfiles and Amazon S3 http://imagerjs.github.io/imager/	1.0.0-alpha1	pkgcloud(0.9.6)<-qs(0.6.x)	stars		
requester(npm,gh)	A simple network request helper that is geared towards crawling. (a few keywords GZIP, XML, JSON, PROXIES)	0.1.20	qs(~0.5.3)	stars		
doxx(npm, gh)	Generic, template based,	0.7.4	marked(~0.2.9)	stars	resolved	Yes

	HTML output for Dox documentation generator http://twitter.com/FGRibreau					
frontail(npm,gh)	realtime log stream in the browser	1.3.0	validator(1.5.0)	stars	Yes!	
replpad(npm,gh)	Pipes content of files to a node repl whenever they change to enable a highly interactive coding experience. http://thlorenz.github.com/replpad/	0.12.0	marked(~0.2.9)	stars		
glog(npm,gh)	git push blog server	1.4.0	marked(~0.2.6)	stars		
percolator(npm,gh)	Percolator is a framework for quickly	1.5.0	detour(0.16.9)<-send(0.1.4)	stars		

	and easily building quality HTTP APIs in Node.js https://github.com/cainus/percolator#readme					
harmonic(npm, gh)	The next static site generator	0.0.9	markdown-extra(^0.1.0)<-marked(~0.2.5)	stars		
spotify-web-api-node(npm, gh)	A Node.js wrapper for Spotify's new Web API.	1.0.2	restler(~3.2.0)->qs(0.6.6)	active		
wordpress-rest-api(npm, gh)	A Node.js-based client for the WordPress JSON API	0.3.0	superagent(^0.18.0)->qs(0.6.6)	active		
couchtato(npm, gh)	CouchDB database iterator tool http://blog.cliffano.com/tag/couchtato/	0.1.6	bagofcli(~0.0.5)<-validator(~1.5.1)	active	No! XSS not used gh update, npm not!! npm latest 2013!	

marked-toc (npm,gh)	Generate a TOC (table of contents) for markdown files. https://github.com/jonschlinkert	0.2.6	marked(0.3.0)	active (deprecated now)		
datagen (npm,gh)	Multi-process test data files generator. http://blog.cliffano.com/tag/datagen/	0.0.10	bagofcli(~0.0.8)<-validator(~1.5.1)	active	No! XSS not used gh update, npm not!! npm latest 2013!	
stardog (npm,gh)	Stardog JavaScript Framework for node.js and the browser - Develop apps using the Stardog RDF Database & JS. http://clarkparsia.github.com/stardog.js	0.1.5	restler(~3.2.0)->qs(0.6.6)	active		
nodeportal	nodeporta	0.2.3	validator(0	active	Yes!	

(npm, gh)	l(NP), inspired from Liferay is Portal platform built on Node.js		.3.9)			
restling (npm, gh)	A nodejs library to make promise based asynchronous http requests.	0.6.4	restler(^3.2.2)->qs(0.6.6)	active		
hotplate(npm, gh)	Framework to create multi-homed SaaS with NodeJs, Express, Dojo	0.3.35	send(0.1.x)	active	resolved	
xpush (npm, gh)	XPUSH is an realtime communication channel server for quickly, easily adding scalable functionality to web and mobile apps. http://xpu	0.0.14	send(^0.6.0)	active		

	sh.github.io/about					
rain(npm, gh)	RAIN is a highly scalable frontend platform that orchestrates distributed rendering of loosely coupled components.	0.34.8	connect(2.2.2)	active		
clever(npm,gh)	Node.js library for the Clever API	0.6.0	quest(~0.2.4)<-qs(~0.5.1)	active		
penguin (npm, gh)	Automatically generates administration pages based on your Mongoose models.	0.2.1	body-parser(~1.5.2)->qs(0.6.6)	active		Yes, but not for the identified dep

webdriver-http-sync(npm,gh)	Sync http implementation of the WebDriver protocol for Node.js	0.10.0	request-sync (0.0.5)<-qs (0.6.6)	active	gh updated, not npm	
livewire(npm, gh)	Livescript microrouting library http://blog.153.io/2014/07/15/building-a-simple-rest-api/	0.6.0	qs(~0.6.6)	active		
bugsnag-notification-plugins (npm,gh)	Notification plugins for the Bugsnag error tracker https://bugsnag.com	1.22.1	qs(~0.6.6)	active		
cabbie(npm,gh)	WebDriver for the masses	0.0.9	request-sync (0.0.5)<-qs (0.6.6)	active	npm not updated, but gh	
voicetext(npm,gh)	VoiceText Web API beta client for node.js	0.0.4	superagent(^0.18.1)->qs(0.6.6)	active		
gifsockets-server(npm,gh)	Never-ending animated	0.38.1	marked(~0.2.10)	active		

	GIFs as a chat system http://gifsockets.twolfson.com/					
node-tvdb(npm,gh)	Node.js library for accessing TheTVDB API https://www.npmjs.org/package/node-tvdb	0.4.2	superagent(^0.18.2)->qs(0.6.6)	active	resolved	
supermarked(npm,gh)	marked with syntax highlighting and LaTeX maths support	1.1.0	marked(~0.2.6)	active	resolved	
netbug(npm, gh)	Network Debugger	2.0.1	connect(2.3.6)	active		
bfydir (npm,gh)	http-server to browserify *.js in a dir https://npmjs.org/package/bfydir	1.0.1	st(0.2.4)	active	dep removed	Yes, local dev
hoist-js(np	The hoist	0.0.8-pre	superagent(^0.18.0	active		

m,gh)	client side library		)->qs(0.6.6)			
sentry-node(npm,gh)	simple node wrapper around the Sentry API	1.0.5	quest(~0.2.4)<-qs(~0.5.1)	active		
pesapaljs(npm,gh)	Integrate PesaPal into your Node application	0.0.2-a	phpjs(1.3.2)<-send(0.1.0)	active		
shipshape(npm,gh)	Local server for communicating with shipshape.io	0.1.23	restler(3.2.2)<-qs(0.6.6)	active		
apostrophe-twitter(npm,gh)	A twitter widget for Apostrophe webpages.	0.5.22	qs(~0.6.5)	active		
amorphic(npm, gh)	A front-to-back isomorphic framework for developing applications with node.js and mongoDB	2.6.2	connect(2.6.2)	active		

node-linkedin-simple (npm,gh)	Node.JS bindings for LinkedIn API	0.0.3	qs(~0.6.5)	active	gh updated, but not npm	Yes, reported and updated
okanjo (npm, gh)	Okanjo Node.js SDK - https://okanjo.com/	0.1.17	qs(~0.6.6)	active		

What are we keen to know about?

- In principle, a security advisory serve as an indication that there is a security vulnerability, however is the functionality of the advisory used? How do the project maintainers find it useful?
- Does the nature of the advisory play an role whether its updated or not, most advisories are not critical in nature
- What is the migration path? removal of dependency, update to a new version
- is the feeling of knowing to not have a vulnerable version, important or whether the functionality is important? -> implies that the advisories have to be more intelligent?
- Why is github only updated and not npm? shows a clear indication that there has to better interplay between these two services
- in the dependency chain? who is to be blame, can we determine where in the chain should update the modules, maybe an alert system for this type of updates. This is particularly useful in large repositories
- the key problems: old projects that are popular, no manoeuvrability of moving to other versions, can we put pressure on updating modules?

what we can conclude is that we need to tool to:

1) intelligent advisories: we should identify code that is vulnerable
2) repository alert system: find modules that can risk being a threat for many modules, this is to avoid such as heart-bleed. By analyzing the dependency chain, we can determine who should do what. We could have a flagging system for library maintainers not doing their job
3) todays advisory systems are too slow, should maybe be integrated in the CI system

Core problems to solve

- overview of outdated modules
    - both indirect and cascading
- what modules are updated on github and not npm?

•