

Dependency Management & Versioning

17-313 Spring 2023

Left-pad (March 22, 2016)

OBSESSIONS

QUARTZ

NPM ERR!

How one programmer broke the internet by deleting a tiny piece of code

THE VERGE

TECH

REVIEWS

REPORT TECH

How an irate developer briefly broke JavaScript

Unpublishing 11 lines of code brought down an open source house of cards

By Paul Miller | @futurepaul | Mar 24, 2016, 4:29pm EDT



SIGN IN

The Register

SOFTWARE

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using



Left-pad (March 22, 2016)

npmjs.org tells me that left-pad is not available (404 page) #4



silkenrance opened this issue on Mar 22, 2016 · 193 comments



silkenrance commented on Mar 21, 2016

When building projects on travis, or when searching for left-pad on npmjs.com, both will report that the package cannot be found.

Here is an excerpt from the travis build log

```
rpm ERR! Linux 3.13.0-40-generic
rpm ERR! argv "/home/travis/.rvm/versions/node/v4.2.2/bin/node" "/home/travis/.rvm/versions/node/v4.2.2/bin/npm"
rpm ERR! node v4.2.2
rpm ERR! npm v1.4.7
rpm ERR! code E404
rpm ERR! 404 Registry returned 404 for GET on https://registry.npmjs.org/left-pad
rpm ERR! 404
rpm ERR! 404 'left-pad' is not in the npm registry.
rpm ERR! 404 You should bug the author to publish it (or use the same yourself!)
rpm ERR! 404 It was specified as a dependency of 'line-numbers'
rpm ERR! 404
rpm ERR! 404 Note that you can also install from a
rpm ERR! 404 tarball, folder, http url, or git url.
rpm ERR! Please include the following file with any support request:
rpm ERR! /home/travis/build/coldrye-es/pings/npm-debug.log
make: *** [deps: Error 1
```

And here is the standard npmjs.com error page <https://www.npmjs.com/package/left-pad>

However, if I remove left-pad from my local npm cache and then reinstall it using npm it will happily install left-pad@0.0.4.

👍 88 🗨️ 3

Left-pad (Docs)

left-pad

String left pad

build unknown

Install

```
$ npm install left-pad
```

Usage

```
const leftPad = require('left-pad')

leftPad('foo', 5)
// => "  foo"

leftPad('foobar', 6)
// => "foobar"

leftPad(1, 2, '0')
// => "01"

leftPad(17, 5, 0)
// => "00017"
```

Install

```
> npm i left-pad
```

Repository

github.com/stevemao/left-pad

Home page

github.com/stevemao/left-pad#readme

Weekly Downloads

2,962,641



Version

1.3.0

License

WTFPL

Unpacked Size

9.75 kB

Total Files

10

Issues

3

Pull Requests

7

Last publish

4 years ago

Left-pad (Source Code)

17 lines (11 sloc) | 222 Bytes

```
1  module.exports = leftpad;
2
3  function leftpad (str, len, ch) {
4    str = String(str);
5
6    var i = -1;
7
8    if (!ch && ch !== 0) ch = ' ';
9
10   len = len - str.length;
11
12   while (++i < len) {
13     str = ch + str;
14   }
15
16   return str;
17 }
```

See also: isArray

5 lines (4 sloc) | 133 Bytes

```
1 var toString = {}.toString;
2
3 module.exports = Array.isArray || function (arr) {
4   return toString.call(arr) === '[object Array]';
5 };
```

isarray

Array#isArray for older browsers and deprecated Node.js versions.

build passing downloads 227M/month



Just use `Array.isArray` directly, unless you need to support those older versions.

Usage

```
var isArray = require('isarray');

console.log(isArray([])); // => true
console.log(isArray({})); // => false
```

Install

```
> npm i isarray
```

Repository

github.com/juliangruber/isarray

Homepage

github.com/juliangruber/isarray

Weekly Downloads

50,913,317

Version	License
2.0.5	MIT

Unpacked Size	Total Files
3.43 kB	4

Issues	Pull Requests
4	3

Dependency Management

- It's hard
- It's mostly a mess (everywhere)
- But it's critical to modern software development

What is a Dependency?

- Core of what most build systems do
 - “Compile” and “Run Tests” is just a fraction of their job
- Examples: Maven, Gradle, NPM, Bazel, ...
- **Foo->Bar**: To build Foo, you may need to have a built version of Bar
- Dependency Scopes:
 - **Compile**: Foo uses classes, functions, etc. defined by Bar
 - **Runtime**: Foo uses an abstract API whose implementation is provided by Bar (e.g. logging, database, network or other I/O)
 - **Test**: Foo needs Bar only for tests (e.g. JUnit, mocks)
- Internal vs. External Dependencies
 - Is Bar also built/maintained by your org or is it pulled from elsewhere using a package manager?

Dependencies: Example

```

152 <dependencyManagement>
153 <dependencies>
154 <dependency>
155   <groupId>com.sismics.docs</groupId>
156   <artifactId>docs-core</artifactId>
157   <version>${project.version}</version>
158 </dependency>
159
160 <dependency>
161   <groupId>com.sismics.docs</groupId>
162   <artifactId>docs-web-common</artifactId>
163   <version>${project.version}</version>
164 </dependency>
165
166 <dependency>
167   <groupId>com.sismics.docs</groupId>
168   <artifactId>docs-web-common</artifactId>
169   <type>test-jar</type>
170   <version>${project.version}</version>
171 </dependency>
172
173 <dependency>
174   <groupId>com.sismics.docs</groupId>
175   <artifactId>docs-web</artifactId>
176   <version>${project.version}</version>
177 </dependency>
178
179 <dependency>
180   <groupId>org.eclipse.jetty</groupId>
181   <artifactId>jetty-server</artifactId>
182   <version>${org.eclipse.jetty.jetty-server.version}</version>
183 </dependency>
184
185 <dependency>
186   <groupId>org.eclipse.jetty</groupId>
187   <artifactId>jetty-webapp</artifactId>
188   <version>${org.eclipse.jetty.jetty-webapp.version}</version>
189 </dependency>

```

Package: git (1:2.17.1-1ubuntu0.9)

fast, scalable, distributed revision control system

Other Packages Related to git

- **depends** + **recommends** • **suggests** - **enhances**
- **git-man** (>= 1:2.17.1-1) [not amd64, i386]
fast, scalable, distributed revision control system (manual pages)
- git-man** (ec 1:2.17.1-1) [amd64, i386]
- git-man** (>= 1:2.17.1) [not amd64, i386]
- git-man** (>= 1:2.17.1) [amd64, i386]
- **libel** (>= 2.90) [not amd64, ppc64el]
CMake Library Shared Libraries
also a virtual package provided by **libc6-udeb**
- libc** (>= 2.17) [amd64, ppc64el]
- **libcurl-gnutls** (>= 7.16.2)
easy-to-use client-side URL transfer library (GnuTLS flavor)
- **liberror-perl**
Perl module for error/exception handling in an OO-ish way
- **libexpat1** (>= 2.0.1)
XML parsing C library - runtime library
- **libpcre3**
PCRE Compatible Regular Expression Library - runtime files
- **perl**
Larry Wall's Practical Extraction and Report Language
- **zlib1g** (>= 1:1.2.0)
compression library - runtime
- + **less**
pager program similar to more
- + **patch**
Apply a diff file to an original
- + **ssh-client**
virtual package provided by **openssh-client**



Where are the dependencies hosted?



- Typically downloaded from dependency servers:
 - Maven Central (<https://repo.maven.apache.org/maven2/>)
 - Ubuntu Packages for Apt (<https://packages.ubuntu.com/>)
 - Python Package Index (<https://pypi.org/>)]
 - NPM Public Registry (<https://registry.npmjs.org/>)
- Packages need a unique identifier
 - Typically a package name (sometimes owner name) and version
- Custom repositories allowed by most package managers
 - Often used for company-internal packages or cache mirroring
 - Note problems with duplicates (same package name in different repositories; some priority order is needed)
- Somebody needs to manage repositories
 - Availability: Repository needs to be running
 - Access Control: Packages should only be published by owners
 - Integrity: Packages should be signed or otherwise verifiable
 - Uniqueness and archival: Only one artifact per version
 - Traceability: Packages can have metadata pointing to source or tests
 - Security: ???



Transitive Dependencies

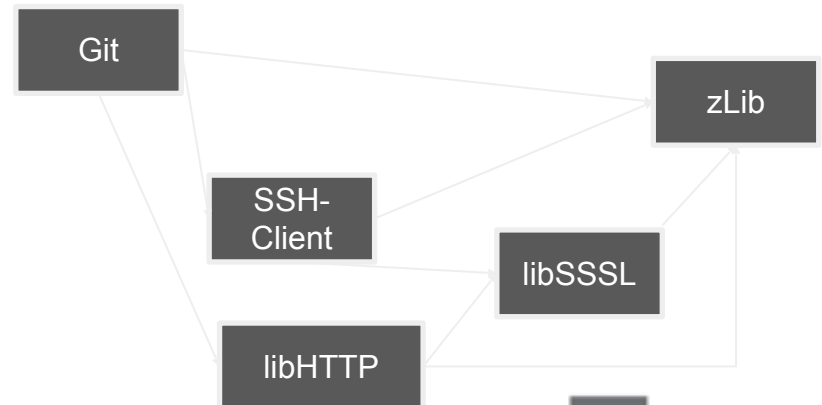
Packages can depend on other packages



Q: Should Git be able to use exports of libSSL (e.g. certificate management) or zLib (e.g. gzip compression)?

Diamond Dependencies

What are some problems when multiple intermediate dependencies have the same transitive dependency?



Diamond Dependencies

What are some problems when multiple intermediate dependencies have the same transitive dependency?



Resolutions to the Diamond Problem

1. Duplicate it!
 - Doesn't work with static linking (e.g. C/C++), but may be doable with Java (e.g. using ClassLoader hacking or package renaming)
 - Values of types defined by duplicated libraries cannot be exchanged across
2. Ban transitive dependencies; just use a global list with one version for each
 - Challenge: Keeping things in sync with latest
 - Challenge: Deciding which version of transitive deps to keep
3. Newest version (keep everything at latest)
 - Requires ordering semantics
 - Intermediate dependency may break with update to transitive
4. Oldest version (lowest denominator)
 - Also requires ordering semantics
 - Sacrifices new functionality
5. Oldest non-breaking version / Newest non-breaking version
 - Requires faith in tests or semantic versioning contract

Semantic Versioning

- Widely used convention for versioning releases
 - E.g. 1.2.1, 3.1.0-alpha-1, 3.1.0-alpha-2, 3.1.0-beta-1, 3.1.0-rc1
- Format: {MAJOR} . {MINOR} . {PATCH}
- Each component is ordered (numerically, then lexicographically; release-aware)
 - 1.2.1 < 1.10.1
 - 3.1.0-alpha-1 < 3.1.0-alpha-2 < 3.1.0-beta-1 < 3.1.0-rc1 < 3.1.0
- Contracts:
 - MAJOR updated to indicate breaking changes
 - Same MAJOR version => backward compatibility
 - MINOR updated for additive changes
 - Same MINOR version => API compatibility (important for linking)
 - PATCH updates functionality without new API
 - Ninja edit; usually for bug fixes

<https://semver.org/>

[2.0.0](#) [2.0.0-rc.2](#) [2.0.0-rc.1](#) [1.0.0](#) [1.0.0-beta](#)

Semantic Versioning 2.0.0

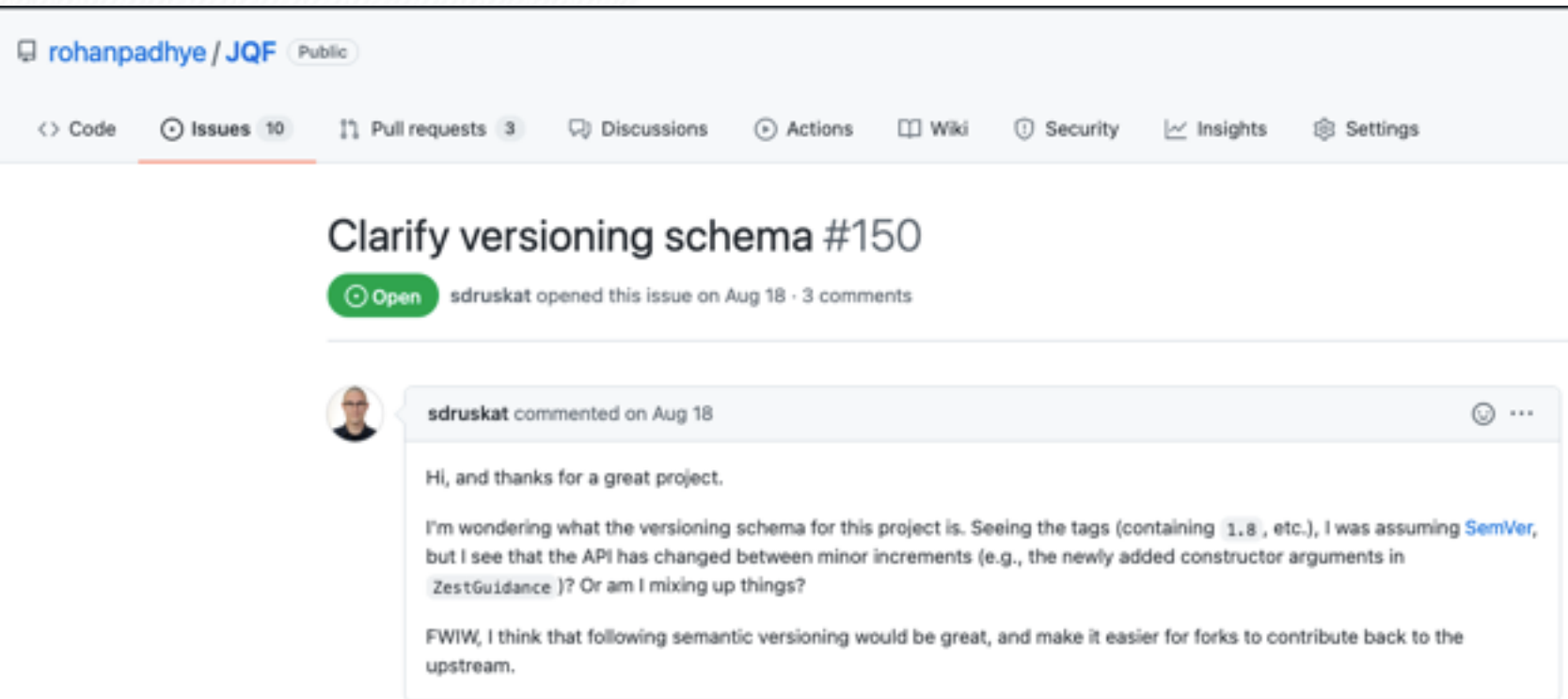
Summary

Given a version number MAJOR.MINOR.PATCH, increment the:

1. MAJOR version when you make incompatible API changes,
2. MINOR version when you add functionality in a backwards compatible manner, and
3. PATCH version when you make backwards compatible bug fixes.

Additional labels for pre-release and build metadata are available as extensions to the MAJOR.MINOR.PATCH format.

People rely on SemVer contracts



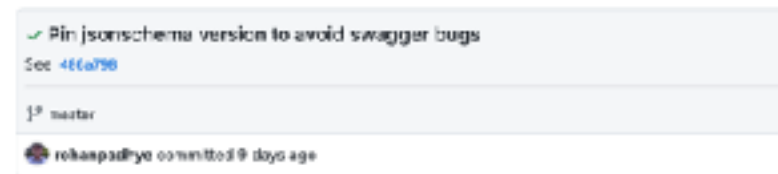
The screenshot shows a GitHub repository page for 'rohanpadhye / JQF'. The navigation bar includes links for Code, Issues (10), Pull requests (3), Discussions, Actions, Wiki, Security, Insights, and Settings. The 'Issues' link is highlighted. Below the navigation bar, the issue title 'Clarify versioning schema #150' is displayed, along with a green 'Open' status and the text 'sdruskat opened this issue on Aug 18 · 3 comments'. A comment from 'sdruskat' is shown, dated 'Aug 18'. The comment text reads: 'Hi, and thanks for a great project. I'm wondering what the versioning schema for this project is. Seeing the tags (containing 1.8 , etc.), I was assuming SemVer, but I see that the API has changed between minor increments (e.g., the newly added constructor arguments in ZestGuidance)? Or am I mixing up things? FWIW, I think that following semantic versioning would be great, and make it easier for forks to contribute back to the upstream.'

Dependency Constraints

- E.g. Declare dependency on "Bar > 2.1"
 - Bar 2.1.0, 2.1.1, 2.2.0, 2.9.0, etc. all match
 - 2.0.x does NOT match
 - 3.0.x does NOT match
- Diamond dependency problem can be resolved using SAT solvers
 - E.g. Foo 1.0.0 depends on "Bar >= 2.1" and "Baz 1.8.x"
 - Bar 2.1.0 depends on "Qux [1.6, 1.7]"
 - Bar 2.1.1 depends on "Qux 1.7.0"
 - Baz 1.8.0 depends on "Qux 1.5.x"
 - Baz 1.8.1 depends on "Qux 1.6.x"
 - Find an assignment such that all dependencies are satisfied
 - Solution: Use Bar 2.1.0, Baz 1.8.1, and Qux 1.6.{latest}

Semantic Versioning Contracts

- Largely trusting developers to maintain them
- Constrained/range dependencies can cause unexpected build failures
- Automatic validation of SemVer is hard



Cyclic Dependencies

- A very bad thing
- Avoid at all costs
- Sometimes unavoidable or intentional
 - E.g. GCC is written in C (needs a C compiler)
 - E.g. Apache Maven uses the Maven build system
 - E.g. JDK tested using JUnit, which requires the JDK to compile



Cyclic Dependencies

- Bootstrapping: Break cycles over time
- Assume older version exists in binary (pre-built form)
- Step 1: Build A using an older version of B
- Step 2: Build B using new (just built) version of A
- Step 3: Rebuild A using new (just built) version of B
- Now, both A and B have been built with new versions of their dependencies
- Doesn't work if both A and B need new features of each other at the same time (otherwise Step 1 won't work)
 - Assumes incremental dependence on new features
- How was the old version built in the first place? (it's turtles all the way down)
 - Assumption: cycles did not exist in the past
 - Successfully applied in compilers (e.g. GCC is written in C)

Dependency Security

- Will you let strangers execute arbitrary code on your laptop?
 - Think about this every time you do “pip install” or “npm install” or “apt-get upgrade” or “brew upgrade” or whatever (esp. with sudo)
 - Scary, right? Who are you trusting? Why?
- Typo squatting (“pip install numpi”)
- Outright malice (remember the *event-stream* incident?)
- Genuine security vulnerabilities due to software bugs

Dependabot alerts #74

Deserialization of Untrusted Data in Apache Log4j #74

[Dismiss alert](#)

[Open](#) [Open in IDE](#) [Log](#) [Log2](#) [Log3](#) [Log4](#) [Log5](#) [Log6](#) [Log7](#) [Log8](#) [Log9](#) [Log10](#) [Log11](#) [Log12](#) [Log13](#) [Log14](#) [Log15](#) [Log16](#) [Log17](#) [Log18](#) [Log19](#) [Log20](#) [Log21](#) [Log22](#) [Log23](#) [Log24](#) [Log25](#) [Log26](#) [Log27](#) [Log28](#) [Log29](#) [Log30](#) [Log31](#) [Log32](#) [Log33](#) [Log34](#) [Log35](#) [Log36](#) [Log37](#) [Log38](#) [Log39](#) [Log40](#) [Log41](#) [Log42](#) [Log43](#) [Log44](#) [Log45](#) [Log46](#) [Log47](#) [Log48](#) [Log49](#) [Log50](#) [Log51](#) [Log52](#) [Log53](#) [Log54](#) [Log55](#) [Log56](#) [Log57](#) [Log58](#) [Log59](#) [Log60](#) [Log61](#) [Log62](#) [Log63](#) [Log64](#) [Log65](#) [Log66](#) [Log67](#) [Log68](#) [Log69](#) [Log70](#) [Log71](#) [Log72](#) [Log73](#) [Log74](#) [Log75](#) [Log76](#) [Log77](#) [Log78](#) [Log79](#) [Log80](#) [Log81](#) [Log82](#) [Log83](#) [Log84](#) [Log85](#) [Log86](#) [Log87](#) [Log88](#) [Log89](#) [Log90](#) [Log91](#) [Log92](#) [Log93](#) [Log94](#) [Log95](#) [Log96](#) [Log97](#) [Log98](#) [Log99](#) [Log100](#) [Log101](#) [Log102](#) [Log103](#) [Log104](#) [Log105](#) [Log106](#) [Log107](#) [Log108](#) [Log109](#) [Log110](#) [Log111](#) [Log112](#) [Log113](#) [Log114](#) [Log115](#) [Log116](#) [Log117](#) [Log118](#) [Log119](#) [Log120](#) [Log121](#) [Log122](#) [Log123](#) [Log124](#) [Log125](#) [Log126](#) [Log127](#) [Log128](#) [Log129](#) [Log130](#) [Log131](#) [Log132](#) [Log133](#) [Log134](#) [Log135](#) [Log136](#) [Log137](#) [Log138](#) [Log139](#) [Log140](#) [Log141](#) [Log142](#) [Log143](#) [Log144](#) [Log145](#) [Log146](#) [Log147](#) [Log148](#) [Log149](#) [Log150](#) [Log151](#) [Log152](#) [Log153](#) [Log154](#) [Log155](#) [Log156](#) [Log157](#) [Log158](#) [Log159](#) [Log160](#) [Log161](#) [Log162](#) [Log163](#) [Log164](#) [Log165](#) [Log166](#) [Log167](#) [Log168](#) [Log169](#) [Log170](#) [Log171](#) [Log172](#) [Log173](#) [Log174](#) [Log175](#) [Log176](#) [Log177](#) [Log178](#) [Log179](#) [Log180](#) [Log181](#) [Log182](#) [Log183](#) [Log184](#) [Log185](#) [Log186](#) [Log187](#) [Log188](#) [Log189](#) [Log190](#) [Log191](#) [Log192](#) [Log193](#) [Log194](#) [Log195](#) [Log196](#) [Log197](#) [Log198](#) [Log199](#) [Log200](#) [Log201](#) [Log202](#) [Log203](#) [Log204](#) [Log205](#) [Log206](#) [Log207](#) [Log208](#) [Log209](#) [Log210](#) [Log211](#) [Log212](#) [Log213](#) [Log214](#) [Log215](#) [Log216](#) [Log217](#) [Log218](#) [Log219](#) [Log220](#) [Log221](#) [Log222](#) [Log223](#) [Log224](#) [Log225](#) [Log226](#) [Log227](#) [Log228](#) [Log229](#) [Log230](#) [Log231](#) [Log232](#) [Log233](#) [Log234](#) [Log235](#) [Log236](#) [Log237](#) [Log238](#) [Log239](#) [Log240](#) [Log241](#) [Log242](#) [Log243](#) [Log244](#) [Log245](#) [Log246](#) [Log247](#) [Log248](#) [Log249](#) [Log250](#) [Log251](#) [Log252](#) [Log253](#) [Log254](#) [Log255](#) [Log256](#) [Log257](#) [Log258](#) [Log259](#) [Log260](#) [Log261](#) [Log262](#) [Log263](#) [Log264](#) [Log265](#) [Log266](#) [Log267](#) [Log268](#) [Log269](#) [Log270](#) [Log271](#) [Log272](#) [Log273](#) [Log274](#) [Log275](#) [Log276](#) [Log277](#) [Log278](#) [Log279](#) [Log280](#) [Log281](#) [Log282](#) [Log283](#) [Log284](#) [Log285](#) [Log286](#) [Log287](#) [Log288](#) [Log289](#) [Log290](#) [Log291](#) [Log292](#) [Log293](#) [Log294](#) [Log295](#) [Log296](#) [Log297](#) [Log298](#) [Log299](#) [Log300](#) [Log301](#) [Log302](#) [Log303](#) [Log304](#) [Log305](#) [Log306](#) [Log307](#) [Log308](#) [Log309](#) [Log310](#) [Log311](#) [Log312](#) [Log313](#) [Log314](#) [Log315](#) [Log316](#) [Log317](#) [Log318](#) [Log319](#) [Log320](#) [Log321](#) [Log322](#) [Log323](#) [Log324](#) [Log325](#) [Log326](#) [Log327](#) [Log328](#) [Log329](#) [Log330](#) [Log331](#) [Log332](#) [Log333](#) [Log334](#) [Log335](#) [Log336](#) [Log337](#) [Log338](#) [Log339](#) [Log340](#) [Log341](#) [Log342](#) [Log343](#) [Log344](#) [Log345](#) [Log346](#) [Log347](#) [Log348](#) [Log349](#) [Log350](#) [Log351](#) [Log352](#) [Log353](#) [Log354](#) [Log355](#) [Log356](#) [Log357](#) [Log358](#) [Log359](#) [Log360](#) [Log361](#) [Log362](#) [Log363](#) [Log364](#) [Log365](#) [Log366](#) [Log367](#) [Log368](#) [Log369](#) [Log370](#) [Log371](#) [Log372](#) [Log373](#) [Log374](#) [Log375](#) [Log376](#) [Log377](#) [Log378](#) [Log379](#) [Log380](#) [Log381](#) [Log382](#) [Log383](#) [Log384](#) [Log385](#) [Log386](#) [Log387](#) [Log388](#) [Log389](#) [Log390](#) [Log391](#) [Log392](#) [Log393](#) [Log394](#) [Log395](#) [Log396](#) [Log397](#) [Log398](#) [Log399](#) [Log400](#) [Log401](#) [Log402](#) [Log403](#) [Log404](#) [Log405](#) [Log406](#) [Log407](#) [Log408](#) [Log409](#) [Log410](#) [Log411](#) [Log412](#) [Log413](#) [Log414](#) [Log415](#) [Log416](#) [Log417](#) [Log418](#) [Log419](#) [Log420](#) [Log421](#) [Log422](#) [Log423](#) [Log424](#) [Log425](#) [Log426](#) [Log427](#) [Log428](#) [Log429](#) [Log430](#) [Log431](#) [Log432](#) [Log433](#) [Log434](#) [Log435](#) [Log436](#) [Log437](#) [Log438](#) [Log439](#) [Log440](#) [Log441](#) [Log442](#) [Log443](#) [Log444](#) [Log445](#) [Log446](#) [Log447](#) [Log448](#) [Log449](#) [Log450](#) [Log451](#) [Log452](#) [Log453](#) [Log454](#) [Log455](#) [Log456](#) [Log457](#) [Log458](#) [Log459](#) [Log460](#) [Log461](#) [Log462](#) [Log463](#) [Log464](#) [Log465](#) [Log466](#) [Log467](#) [Log468](#) [Log469](#) [Log470](#) [Log471](#) [Log472](#) [Log473](#) [Log474](#) [Log475](#) [Log476](#) [Log477](#) [Log478](#) [Log479](#) [Log480](#) [Log481](#) [Log482](#) [Log483](#) [Log484](#) [Log485](#) [Log486](#) [Log487](#) [Log488](#) [Log489](#) [Log490](#) [Log491](#) [Log492](#) [Log493](#) [Log494](#) [Log495](#) [Log496](#) [Log497](#) [Log498](#) [Log499](#) [Log500](#) [Log501](#) [Log502](#) [Log503](#) [Log504](#) [Log505](#) [Log506](#) [Log507](#) [Log508](#) [Log509](#) [Log510](#) [Log511](#) [Log512](#) [Log513](#) [Log514](#) [Log515](#) [Log516](#) [Log517](#) [Log518](#) [Log519](#) [Log520](#) [Log521](#) [Log522](#) [Log523](#) [Log524](#) [Log525](#) [Log526](#) [Log527](#) [Log528](#) [Log529](#) [Log530](#) [Log531](#) [Log532](#) [Log533](#) [Log534](#) [Log535](#) [Log536](#) [Log537](#) [Log538](#) [Log539](#) [Log540](#) [Log541](#) [Log542](#) [Log543](#) [Log544](#) [Log545](#) [Log546](#) [Log547](#) [Log548](#) [Log549](#) [Log550](#) [Log551](#) [Log552](#) [Log553](#) [Log554](#) [Log555](#) [Log556](#) [Log557](#) [Log558](#) [Log559](#) [Log560](#) [Log561](#) [Log562](#) [Log563](#) [Log564](#) [Log565](#) [Log566](#) [Log567](#) [Log568](#) [Log569](#) [Log570](#) [Log571](#) [Log572](#) [Log573](#) [Log574](#) [Log575](#) [Log576](#) [Log577](#) [Log578](#) [Log579](#) [Log580](#) [Log581](#) [Log582](#) [Log583](#) [Log584](#) [Log585](#) [Log586](#) [Log587](#) [Log588](#) [Log589](#) [Log590](#) [Log591](#) [Log592](#) [Log593](#) [Log594](#) [Log595](#) [Log596](#) [Log597](#) [Log598](#) [Log599](#) [Log600](#) [Log601](#) [Log602](#) [Log603](#) [Log604](#) [Log605](#) [Log606](#) [Log607](#) [Log608](#) [Log609](#) [Log610](#) [Log611](#) [Log612](#) [Log613](#) [Log614](#) [Log615](#) [Log616](#) [Log617](#) [Log618](#) [Log619](#) [Log620](#) [Log621](#) [Log622](#) [Log623](#) [Log624](#) [Log625](#) [Log626](#) [Log627](#) [Log628](#) [Log629](#) [Log630](#) [Log631](#) [Log632](#) [Log633](#) [Log634](#) [Log635](#) [Log636](#) [Log637](#) [Log638](#) [Log639](#) [Log640](#) [Log641](#) [Log642](#) [Log643](#) [Log644](#) [Log645](#) [Log646](#) [Log647](#) [Log648](#) [Log649](#) [Log650](#) [Log651](#) [Log652](#) [Log653](#) [Log654](#) [Log655](#) [Log656](#) [Log657](#) [Log658](#) [Log659](#) [Log660](#) [Log661](#) [Log662](#) [Log663](#) [Log664](#) [Log665](#) [Log666](#) [Log667](#) [Log668](#) [Log669](#) [Log670](#) [Log671](#) [Log672](#) [Log673](#) [Log674](#) [Log675](#) [Log676](#) [Log677](#) [Log678](#) [Log679](#) [Log680](#) [Log681](#) [Log682](#) [Log683](#) [Log684](#) [Log685](#) [Log686](#) [Log687](#) [Log688](#) [Log689](#) [Log690](#) [Log691](#) [Log692](#) [Log693](#) [Log694](#) [Log695](#) [Log696](#) [Log697](#) [Log698](#) [Log699](#) [Log700](#) [Log701](#) [Log702](#) [Log703](#) [Log704](#) [Log705](#) [Log706](#) [Log707](#) [Log708](#) [Log709](#) [Log710](#) [Log711](#) [Log712](#) [Log713](#) [Log714](#) [Log715](#) [Log716](#) [Log717](#) [Log718](#) [Log719](#) [Log720](#) [Log721](#) [Log722](#) [Log723](#) [Log724](#) [Log725](#) [Log726](#) [Log727](#) [Log728](#) [Log729](#) [Log730](#) [Log731](#) [Log732](#) [Log733](#) [Log734](#) [Log735](#) [Log736](#) [Log737](#) [Log738](#) [Log739](#) [Log740](#) [Log741](#) [Log742](#) [Log743](#) [Log744](#) [Log745](#) [Log746](#) [Log747](#) [Log748](#) [Log749](#) [Log750](#) [Log751](#) [Log752](#) [Log753](#) [Log754](#) [Log755](#) [Log756](#) [Log757](#) [Log758](#) [Log759](#) [Log760](#) [Log761](#) [Log762](#) [Log763](#) [Log764](#) [Log765](#) [Log766](#) [Log767](#) [Log768](#) [Log769](#) [Log770](#) [Log771](#) [Log772](#) [Log773](#) [Log774](#) [Log775](#) [Log776](#) [Log777](#) [Log778](#) [Log779](#) [Log780](#) [Log781](#) [Log782](#) [Log783](#) [Log784](#) [Log785](#) [Log786](#) [Log787](#) [Log788](#) [Log789](#) [Log790](#) [Log791](#) [Log792](#) [Log793](#) [Log794](#) [Log795](#) [Log796](#) [Log797](#) [Log798](#) [Log799](#) [Log800](#) [Log801](#) [Log802](#) [Log803](#) [Log804](#) [Log805](#) [Log806](#) [Log807](#) [Log808](#) [Log809](#) [Log810](#) [Log811](#) [Log812](#) [Log813](#) [Log814](#) [Log815](#) [Log816](#) [Log817](#) [Log818](#) [Log819](#) [Log820](#) [Log821](#) [Log822](#) [Log823](#) [Log824](#) [Log825](#) [Log826](#) [Log827](#) [Log828](#) [Log829](#) [Log830](#) [Log831](#) [Log832](#) [Log833](#) [Log834](#) [Log835](#) [Log836](#) [Log837](#) [Log838](#) [Log839](#) [Log840](#) [Log841](#) [Log842](#) [Log843](#) [Log844](#) [Log845](#) [Log846](#) [Log847](#) [Log848](#) [Log849](#) [Log850](#) [Log851](#) [Log852](#) [Log853](#) [Log854](#) [Log855](#) [Log856](#) [Log857](#) [Log858](#) [Log859](#) [Log860](#) [Log861](#) [Log862](#) [Log863](#) [Log864](#) [Log865](#) [Log866](#) [Log867](#) [Log868](#) [Log869](#) [Log870](#) [Log871](#) [Log872](#) [Log873](#) [Log874](#) [Log875](#) [Log876](#) [Log877](#) [Log878](#) [Log879](#) [Log880](#) [Log881](#) [Log882](#) [Log883](#) [Log884](#) [Log885](#) [Log886](#) [Log887](#) [Log888](#) [Log889](#) [Log890](#) [Log891](#) [Log892](#) [Log893](#) [Log894](#) [Log895](#) [Log896](#) [Log897](#) [Log898](#) [Log899](#) [Log900](#) [Log901](#) [Log902](#) [Log903](#) [Log904](#) [Log905](#) [Log906](#) [Log907](#) [Log908](#) [Log909](#) [Log910](#) [Log911](#) [Log912](#) [Log913](#) [Log914](#) [Log915](#) [Log916](#) [Log917](#) [Log918](#) [Log919](#) [Log920](#) [Log921](#) [Log922](#) [Log923](#) [Log924](#) [Log925](#) [Log926](#) [Log927](#) [Log928](#) [Log929](#) [Log930](#) [Log931](#) [Log932](#) [Log933](#) [Log934](#) [Log935](#) [Log936](#) [Log937](#) [Log938](#) [Log939](#) [Log940](#) [Log941](#) [Log942](#) [Log943](#) [Log944](#) [Log945](#) [Log946](#) [Log947](#) [Log948](#) [Log949](#) [Log950](#) [Log951](#) [Log952](#) [Log953](#) [Log954](#) [Log955](#) [Log956](#) [Log957](#) [Log958](#) [Log959](#) [Log960](#) [Log961](#) [Log962](#) [Log963](#) [Log964](#) [Log965](#) [Log966](#) [Log967](#) [Log968](#) [Log969](#) [Log970](#) [Log971](#) [Log972](#) [Log973](#) [Log974](#) [Log975](#) [Log976](#) [Log977](#) [Log978](#) [Log979](#) [Log980](#) [Log981](#) [Log982](#) [Log983](#) [Log984](#) [Log985](#) [Log986](#) [Log987](#) [Log988](#) [Log989](#) [Log990](#) [Log991](#) [Log992](#) [Log993](#) [Log994](#) [Log995](#) [Log996](#) [Log997](#) [Log998](#) [Log999](#) [Log1000](#)

Package	Affected versions	Patched versions
log4j-log4j (Maven)	<= 1.2.17	None

CVE-2020-9499 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw v2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.

Users are advised to migrate from `log4j:log4j` to `org.apache.logging.log4j:log4j` for an updated version of the library.

[View details](#) [View code](#) [View logs](#)

Severity: **Critical** 9.8 (10)

CSS base metric	Score
Attack vector	Network
Attack complexity	Low
Privilege required	None
Local access required	None
Scope	Untrusted
Confidentiality	High
Integrity	High
Availability	High

[View details](#) [View code](#) [View logs](#)

Takeaways

- Dependency management is hard.