

Ruby - Bug #18424

Is Ruby is vulnerable to log4j?

12/23/2021 11:05 AM - salamani (Ravi Salamani)

Status:	Rejected	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	master	Backport: 2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN
Description I observed that the ruby uses zookeeper, dep "slyphon-log4j", "= 1.2.15". Is Ruby is vulnerable to log4j?		

History

#1 - 12/23/2021 11:19 AM - mame (Yusuke Endoh)

- Status changed from Open to Rejected

The Ruby package itself does not depend on log4j. For an application or library written in Ruby, please ask to its maintainer.

#2 - 12/23/2021 02:11 PM - salamani (Ravi Salamani)

mame (Yusuke Endoh) wrote in [#note-1](#):

The Ruby package itself does not depend on log4j. For an application or library written in Ruby, please ask to its maintainer.

https://github.com/ruby/ruby/blob/master/spec/bundler/resolver/platform_spec.rb#L31 Does it installs log4j?

#3 - 12/23/2021 02:53 PM - austin (Austin Ziegler)

salamani (Ravi Salamani) wrote in [#note-2](#):

mame (Yusuke Endoh) wrote in [#note-1](#):

The Ruby package itself does not depend on log4j. For an application or library written in Ruby, please ask to its maintainer.

https://github.com/ruby/ruby/blob/master/spec/bundler/resolver/platform_spec.rb#L31 Does it installs log4j?

This is a Ruby spec that verifies bundler. This particular path would only be run by JRuby and possibly TruffleRuby, as CRuby is not written with Java.

#4 - 12/23/2021 05:36 PM - deivid (David Rodríguez)

Yes, that's correct. The naming in these test cases is inspired by realworld packages, but these are just dummy packages just for the sake of testing, not the real library code. You can replace log4j with very-secure-library in those tests and they should still pass.