Redmine - Defect #35949

Several Critical CVEs

2021-10-01 22:07 - Marcelo Simas

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	4.2.2

Description

We use redmine 4.2.2 through a container and the scanner which runs in our DTR has recently identified several critical CVEs. We wanted to make you aware of that.

CVE-2021-23440
Critical
9.8
set-value
2.0.1
4.0.1
No

CVE-2017-6519
Critical
9.1
libavahi-client3
0.7-4+deb10u1
No

CVE-2017-6519
Critical
9.1
libavahi-common-data
0.7-4+deb10u1
No

CVE-2017-6519
Critical
9.1
libavahi-common3
0.7-4+deb10u1
No

CVE-2019-1010022
Critical
9.8
libc-bin
2.28-10
No

CVE-2021-33574
Critical
9.8
libc-bin
2.28-10
No

CVE-2021-35942
Critical
9.1
libc-bin
2.28-10

No

CVE-2019-1010022
Critical
9.8
libc-dev-bin
2.28-10
No

CVE-2021-33574
Critical
9.8
libc-dev-bin
2.28-10
No

CVE-2021-35942
Critical
9.1
libc-dev-bin
2.28-10
No

CVE-2019-1010022
Critical
9.8
libc6
2.28-10
No

CVE-2021-33574
Critical
9.8
libc6
2.28-10
No

CVE-2021-35942
Critical
9.1
libc6
2.28-10
No

CVE-2019-1010022
Critical
9.8
libc6-dev
2.28-10
No

CVE-2021-33574
Critical
9.8
libc6-dev
2.28-10
No

CVE-2021-35942
Critical
9.1
libc6-dev
2.28-10
No

CVE-2020-12268
Critical

9.8
libjbig2dec0
0.16-1
No

CVE-2017-17479
Critical
9.8
libopenjp2-7
2.3.0-2+deb10u2
No

CVE-2018-7648
Critical
9.8
libopenjp2-7
2.3.0-2+deb10u2
No

CVE-2021-3177
Critical
5.9
libpython2.7
2.7.16-2+deb10u1
No

CVE-2021-3177
Critical
9.8
libpython2.7-minimal
2.7.16-2+deb10u1
No

CVE-2021-3177
Critical
5.9
libpython2.7-stdlib
2.7.16-2+deb10u1
No

CVE-2019-9893
Critical
9.8
libseccomp2
2.3.3-4
No

CVE-2020-11656
Critical
9.8
libsqlite3-0
3.27.2-3+deb10u1
No

CVE-2017-9117
Critical
9.8
libtiff5
4.1.0+git191117-2~deb10u2

CVE-2019-25032
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25033
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25034
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25035
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25038
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25039
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2019-25042
Critical
9.8
libunbound8
1.9.0-2+deb10u2
No

CVE-2021-3177
Critical
9.8
python2.7
2.7.16-2+deb10u1
No

CVE-2021-3177
Critical
9.8
python2.7-minimal
2.7.16-2+deb10u1
No

CVE-2020-8165
Critical
9.8
activesupport
5.2.3
6.0.3.1, 5.2.4.3
No

CVE-2019-5477
Critical
9.8

nokogiri
1.10.3
1.10.4
No

CVE-2021-31597
Critical
9.4
xmlhttprequest-ssl
1.5.5
1.6.1
No

History

#1 - 2021-10-02 20:31 - Marius BĂLTEANU

- Status changed from New to Closed

- Resolution set to Invalid

Thanks Marcelo for reporting this issue, but the Docker image is not maintained by us, you should report it to the maintainers.

Which image to you use?

#2 - 2021-10-03 00:31 - Marcelo Simas

- Status changed from Closed to Reopened

I believe some of these vulnerabilities may be in your software. One of them I know is related a npm package which was recently patched. Please consider updating your dependencies to take in recent security patches. It is possible some of the other ones are related to OS packages, but those can be addressed by applying patches as part of the container rebuild.

The image copies Redmine from your release URL. You can see that in its Dockerfile (line 49):

https://github.com/docker-library/redmine/blob/master/4.2/Dockerfile

Thanks for taking the time to consider this.

#3 - 2021-10-11 21:54 - Holger Just

- Status changed from Reopened to Closed

None of the vulnerabilities you have listed are in Redmine. Instead, they are all vulnerabilities of either base software of your Docker image (such as the various lib* vulnerabilities), dependencies maintained outside of Redmine (such as nokogiri) or entirely unrelated software (such as the npm packages). Please be aware that Redmine does not depend on any npm packages and does not require or use nodejs on the server.

In any case, as already written by Marius, the Docker image is not maintained by the Redmine project. As such, we have no insight nor the ability to update the software used by this image. Instead, please contact the maintainers of this Docker image if you think there are pending updates they have not yet included into their Docker image.

#4 - 2021-10-11 22:36 - Marcelo Simas

Thank you for looking into this. I will relay these findings to our security folks.