

# openSUSE Leap 15.1 - action #47561

## Security Audit

2019-02-13 11:34 - Inussel

<b>Status:</b> Resolved	<b>Start date:</b> 2019-04-11
<b>Priority:</b> Normal	<b>Due date:</b> 2019-04-26
<b>Assignee:</b> jsegitz	<b>% Done:</b> 100%
<b>Category:</b> Security	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b> RC	
<b>Description</b> Security needs to take a look at the current snapshot	
<b>Related issues:</b>	
Copied from openSUSE Leap 15.0 - action #24884: Security Audit	<b>Closed</b> <b>2018-04-26</b> <b>2018-05-11</b>
Copied to openSUSE Leap 15.2 - action #61314: Security Audit	<b>Resolved</b> <b>2020-04-02</b> <b>2020-06-16</b>

### History

#### #1 - 2019-02-13 11:35 - Inussel

- Copied from action #24884: Security Audit added

#### #2 - 2019-04-15 08:22 - Inussel

- Assignee set to jsegitz

15.1 enters RC phase this week. time for 2nd round of audit

#### #3 - 2019-04-23 06:34 - jsegitz

- Status changed from New to In Progress

- % Done changed from 0 to 80

almost done from our side. I'm still working on a comparison of the fixes that went into Factory and what we might have missed for 15.1., but that will take a little bit longer anyway. For your planning purposes you can consider this done

#### #4 - 2019-04-24 10:55 - jsegitz

- Status changed from In Progress to Resolved

- % Done changed from 80 to 100

Missing fixes compared to Factory:

Needs checking:

- 389-ds: CVE-2017-15134 CVE-2018-1054 CVE-2018-10850 CVE-2018-10871 CVE-2018-1089 CVE-2018-10935 CVE-2018-14624 CVE-2018-14638 CVE-2018-14648 - gthumb: CVE-2018-18718
- icecast: CVE-2018-18820
- kcodecs: CVE-2013-0779
- python-colander: CVE-2017-18361
- rdesktop: CVE-2018-20174 CVE-2018-20175 CVE-2018-20176 CVE-2018-20177 CVE-2018-20178 CVE-2018-20179 CVE-2018-20180 CVE-2018-20181 CVE-2018-20182 CVE-2018-8791 CVE-2018-8792 CVE-2018-8793 CVE-2018-8794 CVE-2018-8795 CVE-2018-8796 CVE-2018-8797 CVE-2018-8798 CVE-2018-8799 CVE-2018-8800
- rust: CVE-2018-1000622
- taglib: CVE-2017-12678 CVE-2018-11439

maybe needs checking:

- GraphicsMagick: CVE-2016-2317
- NetworkManager-vpnc: CVE-2018-10900
- arc: CVE-2015-9275
- cacti: CVE-2009-4112 CVE-2018-20723 CVE-2018-20724 CVE-2018-20725 CVE-2018-20726
- cobbler: CVE-2017-1000469 CVE-2018-1000225 CVE-2018-1000226 CVE-2018-10931
- docker-distribution: CVE-2017-11468
- epiphany: CVE-2018-11396 CVE-2018-12016
- exim: CVE-2017-1000369 CVE-2017-16943 CVE-2017-16944 CVE-2018-6789
- ffmpeg-4: CVE-2017-17555 CVE-2018-13305

- freeimage: CVE-2015-0852 CVE-2016-5684
- hostapd: CVE-2017-13082 CVE-2018-14526
- leptonica: CVE-2017-18196 CVE-2018-3836 CVE-2018-7186 CVE-2018-7247 CVE-2018-7440 CVE-2018-7441 CVE-2018-7442
- libqt5-qtwebengine: CVE-2018-6033 CVE-2019-5786
- libuser: CVE-2015-3245 CVE-2015-3246
- live555: CVE-2019-7314
- mailman: CVE-2011-0707 CVE-2015-2775 CVE-2018-0618
- matrix-synapse: CVE-2018-12291 CVE-2019-5885
- mbedtls: CVE-2018-19608
- miniupnpc: CVE-2017-1000494
- mobidict: CVE-2018-11724 CVE-2018-11725 CVE-2018-11726
- mp3gain: CVE-2017-12911 CVE-2017-14407
- nagios: CVE-2018-13441 CVE-2018-13457 CVE-2018-13458 CVE-2018-18245
- netdata: CVE-2018-18836 CVE-2018-18837 CVE-2018-18838 CVE-2018-18839
- obs-service-refresh\_patches: CVE-2018-12477
- otrs: CVE-2017-17476 CVE-2018-16586 CVE-2018-19141
- podofu: CVE-2017-7381 CVE-2017-7382 CVE-2017-7383 CVE-2017-8054 CVE-2018-11255 CVE-2018-11256 CVE-2018-12982  
CVE-2018-14320 CVE-2018-20751 CVE-2018-5783
- postgresql96: CVE-2018-10915 CVE-2018-10925 CVE-2018-1115
- proftpd: CVE-2017-7418
- python-Django: CVE-2018-14574 CVE-2018-16984 CVE-2019-3498 CVE-2019-6975
- python-Django1: CVE-2018-14574 CVE-2019-3498 CVE-2019-6975
- python-bokeh: CVE-2017-18342
- python-buku: no CVEs found, please check the diff manually. Usually "CVE" is mentioned somewhere
- python-marshmallow: CVE-2018-17175
- python-ropo: CVE-2014-3539
- python-semantic\_version: no CVEs found, please check the diff manually. Usually "CVE" is mentioned somewhere
- python-slixmpp: CVE-2019-1000021
- python-websockets: CVE-2018-1000518
- rocksndiamonds: CVE-2011-4606
- rubygem-sinatra: CVE-2018-11627
- rust-packaging: no CVEs found, please check the diff manually. Usually "CVE" is mentioned somewhere
- sysdig: no CVEs found, please check the diff manually. Usually "CVE" is mentioned somewhere
- tcpreplay: CVE-2018-17580 CVE-2018-17582 CVE-2018-17974 CVE-2018-18407 CVE-2018-18408 CVE-2019-8376 CVE-2019-8377  
CVE-2019-8381
- thttpd: CVE-2017-17663
- tmux: CVE-2018-19387
- ufraw: CVE-2015-8366 CVE-2018-19655
- vdr: no CVEs found, please check the diff manually. Usually "CVE" is mentioned somewhere
- wesnoth: CVE-2018-1999023
- znc: CVE-2019-9917

I'm going to weed out false positives and hand the remaining issues to reactive security for checking

##### #5 - 2019-12-20 13:00 - Inussel

- Copied to action #61314: Security Audit added