Managing a database of vulnerabilities for a package system: the pkgsrc study case

Leonardo Taccari
<leot@NetBSD.org>

The NetBSD Foundation

ITASEC20, February 7th 2020, Ancona, Italy

NetBSD

«NetBSD is a free, fast, secure, and highly portable Unix-like Open Source operating system. It is available for a wide range of platforms, from large-scale servers and powerful desktop systems to handheld and embedded devices.» [1]

[1] From `https://www.NetBSD.org/`

pkgsrc

«pkgsrc is a framework for building third-party software on NetBSD and other UNIX-like systems, currently containing over 22,500 packages. It is used to enable freely available software to be configured and built easily on our 23 supported platforms.» [2]

[2] From `https://www.pkgsrc.org/`

pkgsrc: installing binary packages, bootstrap and building packages

- To install pre-built binary packages, after the `PKG_PATH` environment variable is set to an URL containing binary packages, e.g. to install Tor and all its dependencies:

```
# pkg_add tor
```

- To bootstrap pkgsrc (build and install required tools (e.g. `bmake`) and `pkg_install` tools):

```
$ cvs -danoncvs@anoncvs.NetBSD.org:/cvsroot \
    checkout pkgsrc
$ cd pkgsrc/bootstrap
$ ./bootstrap
```

- To build and install a package and all its dependencies from source, e.g. Tor:

```
$ cd pkgsrc/net/tor
$ bmake install
```

pkgsrc: security

package signatures	binary packages can be cryptographically signed via GPG and the corresponding signature can be verified when installing them via `pkg_add`
Stack Smashing Protection (SSP)	aims to reduce the impact and exploitability of buffer overflow vulnerabilities
Fortify	technique to automatically adding boundary checks where possible
`pkg-vulnerabilities`	database of all known - fixed and not fixed - vulnerabilities and end-of-life packages

pkg-vulnerabilities

`pkg-vulnerabilities` is a text file (TSV) containing a 3-uple of package vulnerabilities entries in the following format, one entry per line:

package	`PKGNAME` patterns [3]
type of exploit	(e.g. `denial-of-service`, `buffer-overflow`, `multiple-vulnerabilities`, `eol`, ...)
URL	URL that contains details about the vulnerability (often nvd.nist.gov for CVEs)

[3] In case of doubt, `pkg_admin pmatch pattern pkg` can be used and returns true if 'pkg' matches 'pattern', e.g.
`pkg_admin pmatch 'foo<1.0' 'foo-1.0'` will return false.

An excerpt from pkg-vulnerabilities

```
# $NetBSD: pkg-vulnerabilities,v 1.9854 2020/01/28 13:31:09 tpaul Exp $
#
#FORMAT 1.0.0
#
# Note: If this file format changes, please do not forget to update
# pkgsrc/mk/scripts/genreadme.awk which also parses this file.
#
# Note: NEVER remove entries from this file; this should document *all*
# known package vulnerabilities so it is entirely appropriate to have
# multiple entries in this file for a single package, and to contain
# entries for packages which have been removed from pkgsrc.
#
# New entries should be added at the end of this file.
#
# Please ask pkgsrc-security to update the copy on ftp.NetBSD.org after
# making changes to this file.
#
# The command to run for this update is "./pkg-vuln-update.sh", but it needs
# access to the private GPG key for pkgsrc-security.
#
# If you have comments/additions/corrections, please contact
# pkgsrc-security@NetBSD.org.
#
# package                       type of exploit          URL
[...]
qemu-[0-9]*                     heap-overflow            https://nvd.nist.gov/vuln/detail/CVE-2020-7039
samba>=4.9<4.11.5               use-after-free           https://nvd.nist.gov/vuln/detail/CVE-2019-19344
samba>=4.0<4.11.5               out-of-bounds-read       https://nvd.nist.gov/vuln/detail/CVE-2019-14907
samba>=4.0<4.11.5               improper-access-control  https://nvd.nist.gov/vuln/detail/CVE-2019-14902
libxml2<2.9.10nb1               memory-leak              https://nvd.nist.gov/vuln/detail/CVE-2019-20388
libxml2<2.9.10nb1               denial-of-service        https://nvd.nist.gov/vuln/detail/CVE-2020-7595
py{27,36,37,38}-waitress<1.4.0 http-request-smuggling   https://nvd.nist.gov/vuln/detail/CVE-2019-16792
webkit-gtk<2.26.3               multiple-vulnerabilities https://webkitgtk.org/security/WSA-2020-0001.html
```

pkg_admin(1) and vulnerabilities

pkg_admin(1) has several commands to inform users about vulnerable packages:

audit
: print a list of vulnerabilities for all installed packages. On NetBSD, if the check_pkg_vulnerabilities option is set, this is enabled by default, the daily(5) cron job will list all vulnerability packages installed.

audit-pkg
: like audit but only print a list of vulnerabilities for given package names or patterns

audit-history
: print all vulnerabilities for the given base package names

fetch-pkg-vulnerabilities
: fetch a new pkg-vulnerabilities file. On NetBSD, this is disabled by default, by adding fetch_pkg_vulnerabilities=YES in /etc/daily.conf the daily(5) cron job will automatically update pkg-vulnerabilities every day.

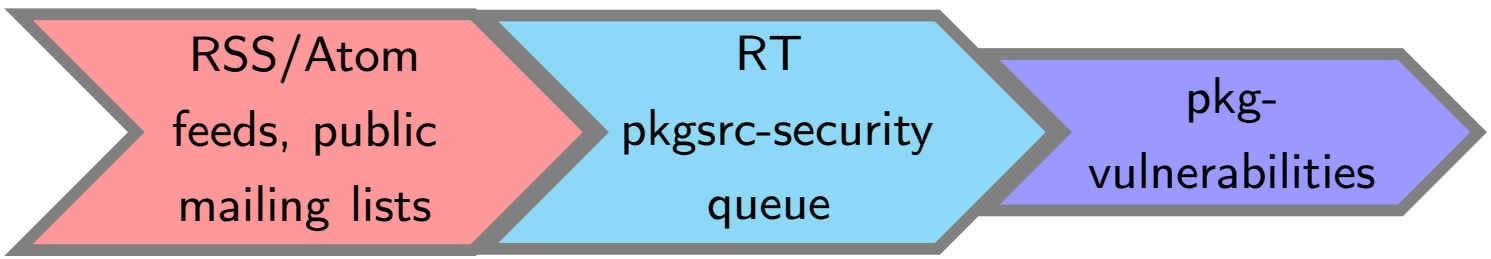
pkg_admin audit in action

```
% pkg_admin audit
Package pcre-8.43 has a denial-of-service vulnerability,
    see https://nvd.nist.gov/vuln/detail/CVE-2017-11164
Package gd-2.2.5nb5 has a double-free vulnerability,
    see https://nvd.nist.gov/vuln/detail/CVE-2019-6978
Package gd-2.2.5nb5 has a double-free vulnerability,
    see https://nvd.nist.gov/vuln/detail/CVE-2019-6978
Package python38-3.8.1nb1 has a crlf-attack vulnerability,
    see https://nvd.nist.gov/vuln/detail/CVE-2019-18348
[...]
```

pkgsrc Security Team

- The mission of pkgsrc Security Team is:
  - ensure that packages in pkgsrc are safe
  - be sure pkgsrc users are aware of the known vulnerabilities in packages
- To track vulnerabilities the Request Tracker (RT) ticket tracking system is used
- A subset of the pkgsrc Security Team members are part of a rotation list:
  - each person is 'on' from Tuesday till Monday
  - ensure that all tickets get handled as soon as possible:
    - reject the ones not affecting pkgsrc
    - add entries to `pkg-vulnerabilities`
    - inform the MAINTAINER (if any)

How pkgsrc-security RT queue and pkg-vulnerabilities are populated?



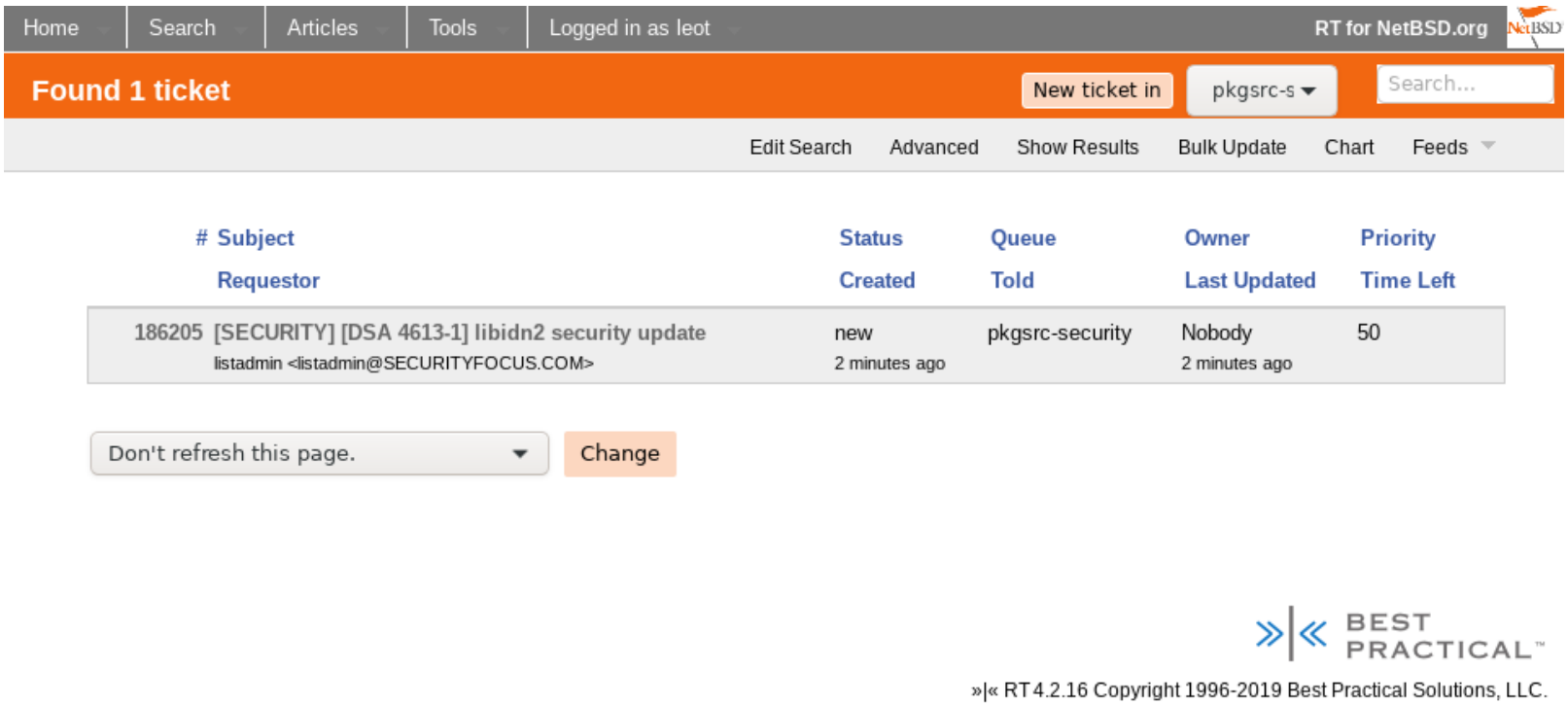
RT ticket statuses used by pkgsrc-security@

new	new (unhandled) ticket
rejected	duplicate issues and ones that do not apply to pkgsrc
resolved	ticket that impacts pkgsrc, entry added to `pkg-vulnerabilities` and mail sent to package `MAINTAINER` (if any)

Ticket handling worflow

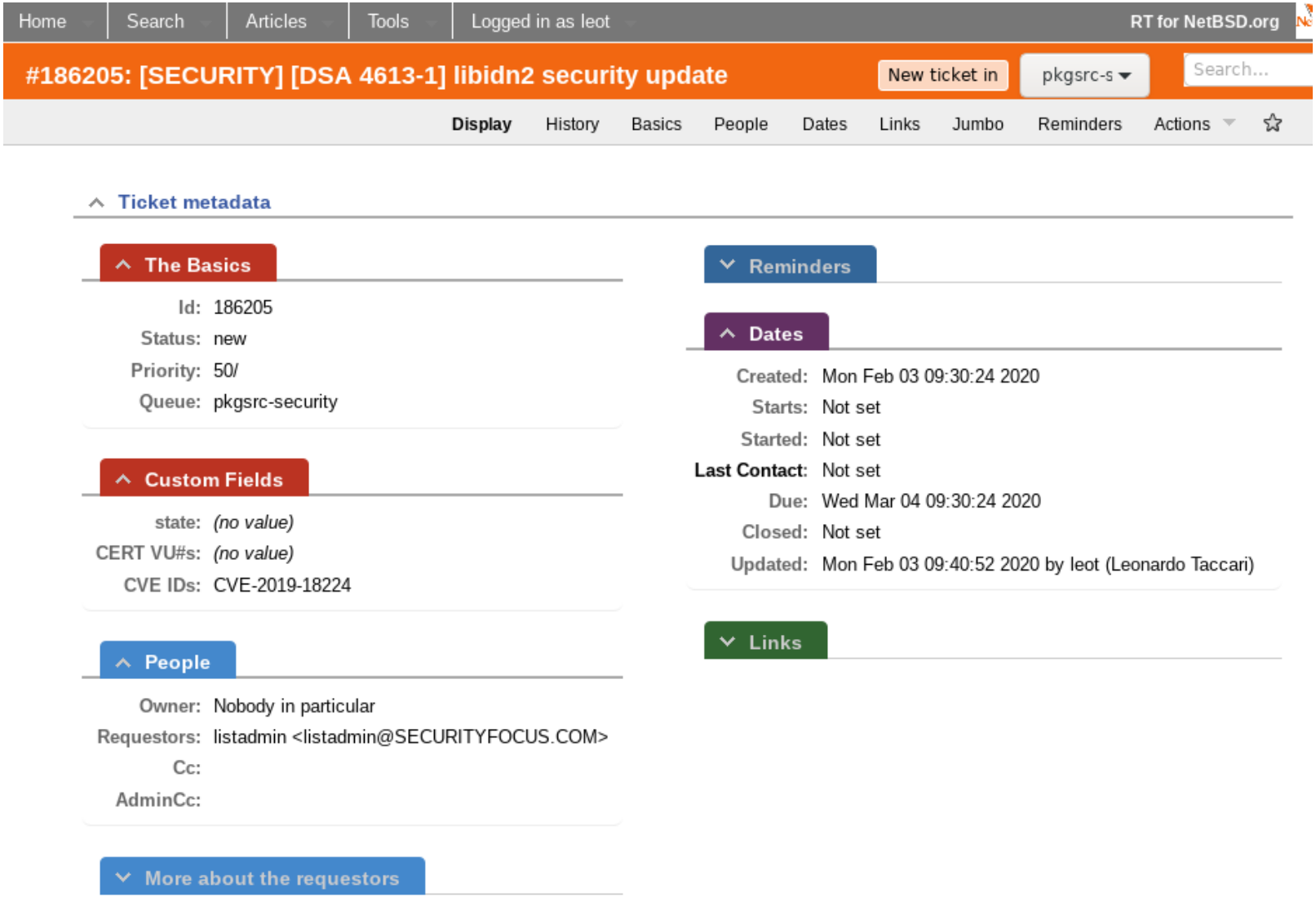
- A **new** ticket arrives in the pkgsrc-security RT queue
- Is the ticket a duplicate?
  - Mark its status as **rejected**
  - Add a 'duplicate' comment
- Does the ticket *not* apply to pkgsrc package(s)?
  - Mark its status as **rejected** and
  - Add a 'No impact on pkgsrc' comment.
- Does the ticket apply to pkgsrc packages(s)?
  - Add an entry to `pkg-vulnerabilities`
  - Upload the new `pkg-vulnerabilities` file
  - Mark its status as **resolved** and
  - Add a 'Entry added to `pkg-vulnerabilities`' comment.
  - Contact `MAINTAINER` (if any)

RT tickets (web interface)



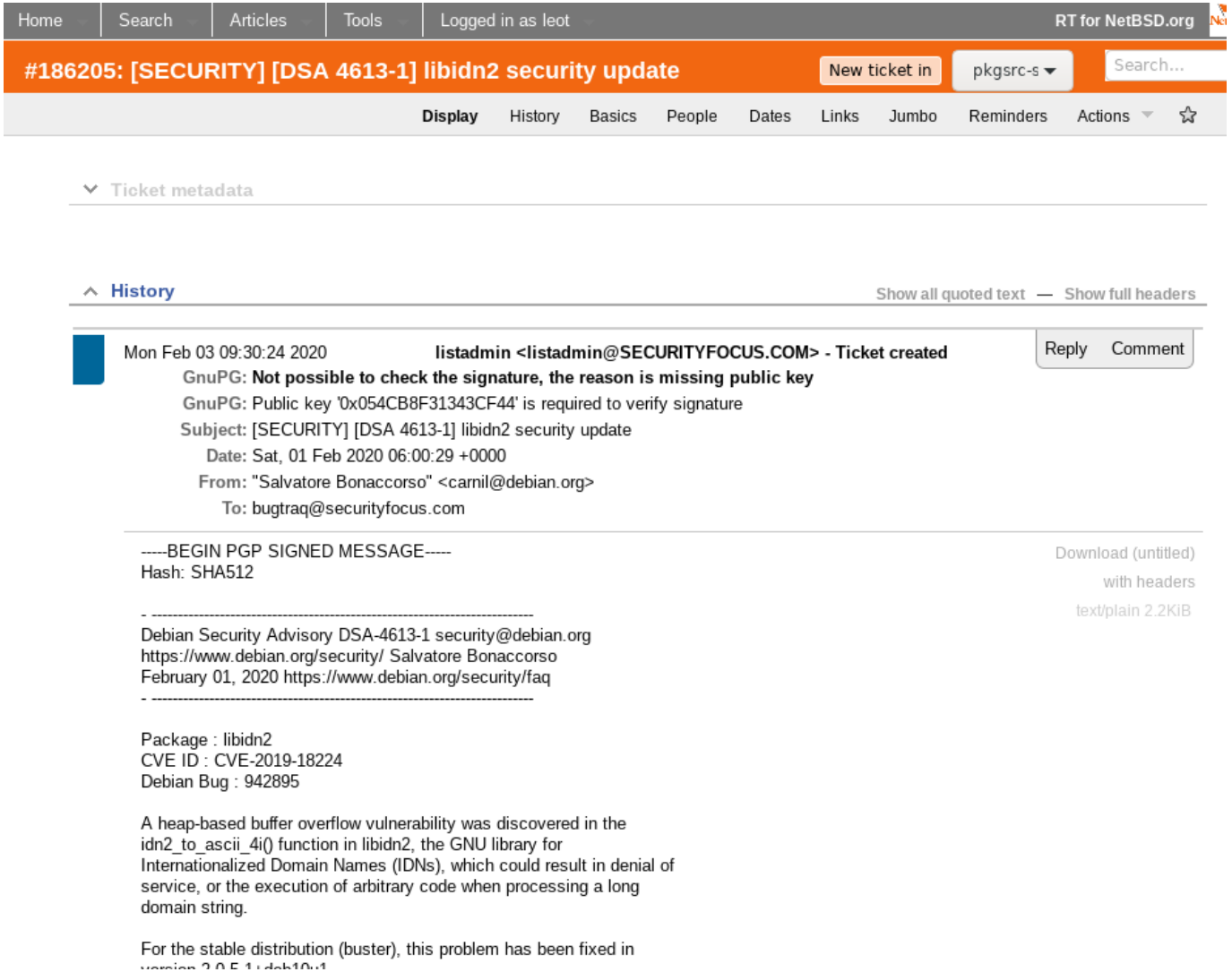
Screenshot of new RT tickets for the pkgsrc-security queue

RT ticket #186205 – DSA 4613-1



Screenshot of new RT ticket #186205, DSA 4613-1 (metadata)

RT ticket #186205 – DSA 4613-1



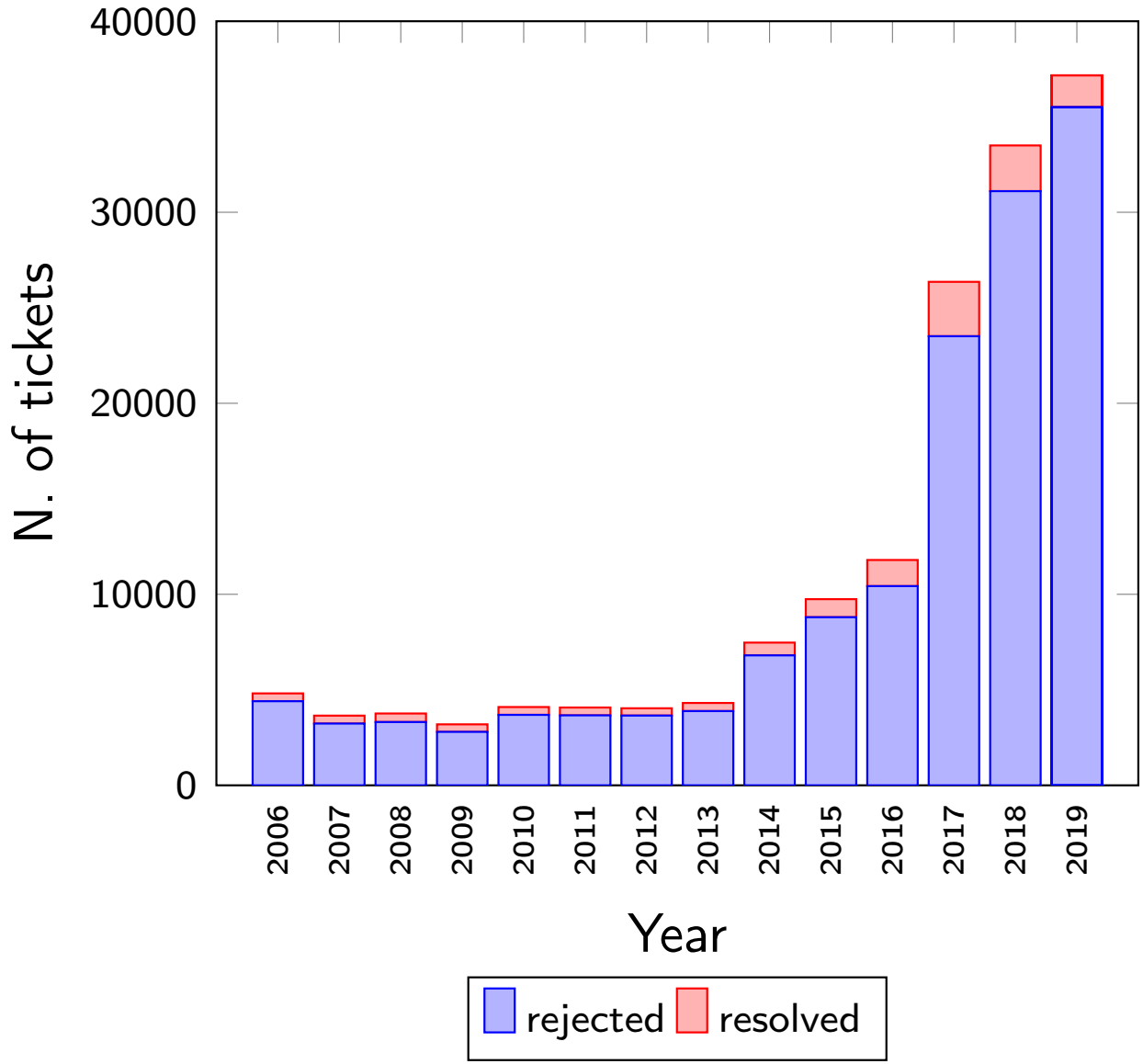
Screenshot of new RT ticket #186205, DSA 4613-1 (history)

Top 10 pkg-vulnerabilities entry types

N. of entries in pkg-vulnerabilities	Type
4823	denial-of-service
1621	multiple-vulnerabilities
1191	arbitrary-code-execution
1036	cross-site-scripting
826	remote-code-execution
631	buffer-overflow
519	privilege-escalation
473	heap-overflow
460	information-disclosure
407	security-bypass

Data from pkg-vulnerabilites of 2020-02-06 (rev. 1.9875).

Tickets through the years



On Jun 19, 2015, RSS feed of nvd.nist.gov is used instead of Secunia Research Advisories.

Caveats, tips, lessons learned

- For CVEs, CPE (common platform enumeration) is often inexact/missing. If no version is present in the description or it says, e.g. '*through* version 1.2.3' instead of '*before* version 1.2.3', always check references for exact versions
- For CVEs, when there is no useful information in references, it is always worth to check Debian Security Bug Tracker, i.e. `https://security-tracker.debian.org/tracker/<CVE>` (where CVE is the corresponding CVE identifier, e.g. CVE-2020-12345)
- Handling hundreds of tickets per week can be stressful: make sure to have an interface comfortable to handle that [6] and have several members handling them

[6] I prefer to read them in the MUA and mark all ones that should be rejected and ones affecting pkgsrc with an (MH) sequence and then push such information to RT via a script using its REST interface.

References I

Alistair Crooks, Hubert Feyrer, The pkgsrc Developers.
The pkgsrc guide.
https://www.NetBSD.org/docs/pkgsrc/.

Pierre Pronchery.
Hardening pkgsrc.
https://www.NetBSD.org/gallery/presentations/khorben/asiabsdcon2017/Hardening%20pkgsrc.html, 2017.
AsiaBSDCon 2017.

pkg-vulnerabilities.
https://ftp.NetBSD.org/pub/NetBSD/packages/vulns/pkg-vulnerabilities.

References II

Alistair G. Crooks.
Changes to the NetBSD Packages Collection in September 2000.
https://mail-index.NetBSD.org/tech-pkg/2000/10/23/0015.html, October 2000.
Initial announcement of audit-packages, precursor of pkg_admin audit command.

Adrian Portelli.
pkgsrc Security.
https://www.pkgsrc.org/pkgsrcCon/2005/slides/adrianp/pkgsrc-Security.html, May 2005.
pkgsrcCon 2005.

Best Practical Solutions, LLC.
Request Tracker.
https://bestpractical.com/request-tracker.

References III

Request Tracker Wiki.
REST - Request Tracker Wiki.
https://rt-wiki.bestpractical.com/wiki/REST.

Debian Security Bug Tracker.
https://security-tracker.debian.org/tracker.

NVD Data Feeds.
https://nvd.nist.gov/vuln/data-feeds.

CVE Web Form.
https://cveform.mitre.org/, a.

CVE Automation Working Group Git Pilot.
https://github.com/CVEProject/cvelist, b.

Questions?

: leot@NetBSD.org