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

¹From 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.»

\(^2\)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

- 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)
```

---

3In 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.
# package type of exploit URL

<table>
<thead>
<tr>
<th>package</th>
<th>type of exploit</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>qemu-[0-9]*</td>
<td>heap-overflow</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2020-7039">https://nvd.nist.gov/vuln/detail/CVE-2020-7039</a></td>
</tr>
<tr>
<td>samba&gt;=4.9&lt;4.11.5</td>
<td>use-after-free</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-19344">https://nvd.nist.gov/vuln/detail/CVE-2019-19344</a></td>
</tr>
<tr>
<td>samba&gt;=4.0&lt;4.11.5</td>
<td>out-of-bounds-read</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-14907">https://nvd.nist.gov/vuln/detail/CVE-2019-14907</a></td>
</tr>
<tr>
<td>samba&gt;=4.0&lt;4.11.5</td>
<td>improper-access-control</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-14902">https://nvd.nist.gov/vuln/detail/CVE-2019-14902</a></td>
</tr>
<tr>
<td>libxml2&lt;2.9.10nb1</td>
<td>memory-leak</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-20388">https://nvd.nist.gov/vuln/detail/CVE-2019-20388</a></td>
</tr>
<tr>
<td>libxml2&lt;2.9.10nb1</td>
<td>denial-of-service</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-7595">https://nvd.nist.gov/vuln/detail/CVE-2019-7595</a></td>
</tr>
<tr>
<td>py{27,36,37,38}-waitress&lt;1.4.0</td>
<td>http-request-smuggling</td>
<td><a href="https://nvd.nist.gov/vuln/detail/CVE-2019-16792">https://nvd.nist.gov/vuln/detail/CVE-2019-16792</a></td>
</tr>
</tbody>
</table>
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?

RSS/Atom feeds, public mailing lists -> RT pkgsrc-security queue -> pkg-vulnerabilities
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 workflow

- 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)
### Ticket metadata

#### History

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Author</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Feb 03 09:30:24 2020</td>
<td></td>
<td>listadmin <a href="mailto:listadmin@SECURITYFOCUS.COM">listadmin@SECURITYFOCUS.COM</a></td>
<td>Ticket created</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GnuPG: Not possible to check the signature, the reason is missing public key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GnuPG: Public key '0x054CB8F3134CF44' is required to verify signature</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Subject: [SECURITY] [DSA 4613-1] libidn2 security update</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Date: Sat, 01 Feb 2020 06:00:29 +0000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>From: &quot;Salvatore Bonaccorso&quot; <a href="mailto:camil@debian.org">camil@debian.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To: <a href="mailto:bugtran@securityfocus.com">bugtran@securityfocus.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---BEGIN PGP SIGNED MESSAGE---

Hash: SHA512

Debian Security Advisory DSA-4613-1 security@debian.org
https://www.debian.org/security/ Salvatore Bonaccorso
February 01, 2020 https://www.debian.org/security/faq

Package : libidn2
CVE ID : CVE-2019-18224
Debian Bug : 942895

A heap-based buffer overflow vulnerability was discovered in the idn2_to_ascii_4() function in libidn2, the GNU library for Internationalized Domain Names (IDNs), which could result in denial of service, or the execution of arbitrary code when processing a long domain string.

For the stable distribution (buster), this problem has been fixed in version 0.3.13-1deb9.4

### Screenshot of new RT ticket #186205, DSA 4613-1 (history)
## Top 10 `pkg-vulnerabilities` entry types

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

Data from `pkg-vulnerabilities` 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 and have several members handling them

6I 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.
Alistair Crooks, Hubert Feyrer, The pkgsrc Developers.  
The pkgsrc guide.  

Pierre Pronchery.  
Hardening pkgsrc.  
AsiaBSDCon 2017.  

pkg-vulnerabilities.  
References II

Alistair G. Crooks.  
Changes to the NetBSD Packages Collection in September 2000.  
Initial announcement of audit-packages, precursor of pkg_admin audit command.

Adrian Portelli.  
pkgssrc Security.  
pkgsCon 2005.

Best Practical Solutions, LLC.  
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.

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

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

✉️: leot@NetBSD.org