

Handling the workflow of pkgsrc Security Team

An introduction to nmh (new MH message system), a look to the workflow of pkgsrc Security Team and how to (possibly) automate the automatable stuffs!

Leonardo Taccari

<leot@NetBSD.org>

The NetBSD Foundation

pkgsrcCon 2018, July 7th 2018, Berlin, Germany



Outline

An introduction to nmh (New Message Handler)

- MH Mail System and nmh new MH message system

- MH mailbox format

- Practical look of a subset of nmh commands

pkgsrc Security Team tasks and workflow

- About pkgsrc Security Team

- pkgsrc-security@ rotation list tasks

- pkgsrc-security RT queue

- pkg_admin and pkg-vulnerabilities

Automating the automatable stuffs of pkgsrc-security

- Programmatic ways to access RT

- Automating ticket handling via the MUA

An introduction to nmh (New Message Handler)

MH Mail System

- ▶ Initially developed in 1978 at RAND
- ▶ MH two main design decisions:
 - ▶ MH commands - the primitive operations on a message - are UNIX shell commands
 - ▶ Each MH message is a normal UNIX file
- ▶ Ease (ab)using the handling of emails via Unix shell scripting

nmh (new MH message system)

- ▶ Based on MH version 6.8.3
- ▶ Available under `modified-bsd` LICENSE
- ▶ Very nice and friendly community!
- ▶ Intended to be a compatible drop-in replacement for MH
- ▶ Suite of simple single-purpose programs to send, receive, save, retrieve and manipulate email messages
- ▶ Available in `pkgsrc` as `mail/nmh`

nmh (new MH message system): MH mailbox format

- ▶ Every email message is just a file (e.g. 123) in a folder ¹ (e.g. pkgsrc-users)
- ▶ Most nmh commands operates on a folder (e.g. +pkgsrc-users) and a range of messages (e.g. 123)
- ▶ Current folder can be omitted and is stored in the user's context ('mhp`ath` +'/ 'mhparam context') ²
- ▶ Current message can be omitted and is stored in folder mh-sequences file ('mhp`ath`'/ 'mhparam mh-sequences') ³
- ▶ Per-folder mh-sequences is also used to:
 - ▶ Special Unseen-Sequence to mark unread messages
 - ▶ Mark a range of messages with a user defined sequence

¹A directory in the file system

²E.g. In ~/Mail/.context: Current-Folder: pkgsrc-users

³E.g. In ~/Mail/pkgsrc-users/.mh_sequences: cur: 123

Practical look of a subset of nmh commands

- `scan` produce a summary listing of nmh messages
- `show` display nmh messages
- `prev` show the previous nmh message
- `next` show the next nmh message
- `folder` set current nmh folder
 - `new` report on nmh folders with new messages
 - `fprev` set current nmh folder to previous folder with new messages
 - `fnext` set current nmh folder to next folder with new messages
- `unseen` scan any new messages in all nmh folders
 - `pick` search nmh messages
 - `mark` manipulate nmh message sequences
 - `comp` compose an nmh message
 - `repl` reply to an nmh message

Subset of nmh commands: scan

*«scan produces a one-line-per-message listing of the specified folder or messages. Each scan line contains the message number (name), the date, the “From:” field, the “Subject” field, and, if room allows, some of the body of the message.»*⁴

```
scan [-help] [-version] [+folder] [msgs] [-clear | -noclear] [-form
formatfile] [-format string] [-header | -noheader] [-width
columns] [-reverse | -noreverse] [-file filename]
```

```
% scan +pkgsrc-changes last:5
N 68024 Jonathan Perkin   Thu Jun 28 15:16 CVS commit: pkgsrc/textproc/ruby-nokogiri
N 68025 Takahiro Kambe    Thu Jun 28 15:33 CVS commit: pkgsrc/security/py-acme
N 68026 Takahiro Kambe    Thu Jun 28 15:34 CVS commit: pkgsrc/doc
N 68027 Jonathan Perkin   Thu Jun 28 15:45 CVS commit: pkgsrc/www/libwww
>N 68028 Greg Troxel       Thu Jun 28 19:00 CVS commit: pkgsrc/ham/rtl-sdr
```

⁴From scan(1)

Subset of nmh commands: show

«show lists each of the specified messages to the standard output (typically, the terminal).»⁵

```
show [-help] [-version] [+folder] [msgs] [-draft] [-showproc program]
[-showmimeproc program] [-header | -noheader] [-checkmime |
-nocheckmime] [-concat | -noconcat] [switches for showproc or
showmimeproc]
```

```
% show +pkgsrc-users 6391
Date: Tue, 19 Jun 2018 16:20:24 +0200
To: pkgsrc-users%netbsd.org@localhost
From: Thomas Merkel <tm%netbsd.org@localhost>
Subject: pkgsrcCon 2018 in Berlin, 6.-8. July
```

Dear pkgsrc users and contributors,

this is a friendly reminder about the pkgsrcCon which takes place in Berlin this year. If you like to present a talk, please send the title, slot duration and brief description for the website to pkgsrcCon2018@NetBSD.org.
[...]

⁵From `show(1)`

Subset of nmh commands: `prev`

«prev performs a show on the previous message in the specified (or current) folder. [...] This command is almost exactly equivalent to “show prev”.»⁶

```
prev [-help] [-version] [+folder] [-showproc program] [-showmimeproc  
program] [-header | -noheader] [-checkmime | -nocheckmime]  
[switches for showproc or showmimeproc]
```

⁶From `prev(1)`

Subset of nmh commands: next

«next performs a show on the next message in the specified (or current) folder. [...] This command is almost exactly equivalent to “show next”.»⁷

```
next [-help] [-version] [+folder] [-showproc program] [-showmimeproc  
program] [-header | -noheader] [-checkmime | -nocheckmime]  
[switches for showproc or showmimeproc]
```

⁷From next(1)

Subset of nmh commands: folder

«When folder is given the `-print` switch (the default), it lists: the current folder, the number of messages in it and their range (low-high), the folder's current message, and an indication of extra files, if any.»⁸

```
folder [-help] [-version] [+folder] [msg] [-all | -noall] [-create |
-nocreate] [-fast | -nofast] [-header | -noheader] [-recurse |
-norecurse] [-total | -nototal] [-list | -nolist] [-push | -pop]
[-pack | -nopack] [-print] [-verbose | -noverbose]
```

folders is equivalent to folder -all

```
% folder
pkgsrc-changes+ has 68011 messages (1-68030); cur=68028.
```

```
% folder -fast
pkgsrc-changes
```

```
% folder -all
FOLDER                # MESSAGES  RANGE          ; CUR          (OTHERS)
[...]
pkgsrc-bugs            has 9378 messages ( 1- 9379); cur= 9379.
pkgsrc-bulk            has 5204 messages ( 1- 5204); cur= 5204.
pkgsrc-changes+       has 68011 messages ( 1-68031); cur=68030.
[...]
```

```
TOTAL = 363611 messages in 144 folders.
```

⁸From folder(1)

Subset of nmh commands: `new`

*«new, in its default mode, produces a one-line-per-folder listing of all folders which contain messages in the specified sequences, or in the sequence(s) listed in the profile entry “Unseen-Sequence”. Each line consists of the folder name, the total number of messages in the specified sequences, and a list of messages derived from the .mh_sequence file.»*⁹

```
new [-help] [-version] [sequences] [-mode mode] [-folders foldersfile]
```

```
fnext is equivalent to new -mode fnext
```

```
fprev is equivalent to new -mode fprev
```

```
unseen is equivalent to new -mode unseen
```

```
% new
netbsd-source-changes      1.  40500
pkgsrc-changes             2.  68029-68030
pkgsrc-wip-changes        1.  10349
total                      4.
```

⁹From `new(1)`

Subset of nmh commands: `fprev`

*«In `fnext` and `fprev` modes, new changes to the next or previous matching folder, respectively.»*¹⁰

```
new [-help] [-version] [sequences] [-mode mode] [-folders foldersfile]
```

```
fnext is equivalent to new -mode fnext
```

```
fprev is equivalent to new -mode fprev
```

```
unseen is equivalent to new -mode unseen
```

```
% fprev
```

```
netbsd-source-changes 40500
```

```
% fprev
```

```
pkgsrc-changes 68029-68030
```

¹⁰From `fprev(1)`

Subset of nmh commands: `fnext`

*«In `fnext` and `fprev` modes, new changes to the next or previous matching folder, respectively.»*¹¹

```
new [-help] [-version] [sequences] [-mode mode] [-folders foldersfile]
```

```
fnext is equivalent to new -mode fnext
```

```
fprev is equivalent to new -mode fprev
```

```
unseen is equivalent to new -mode unseen
```

```
% fnext
```

```
pkgsrc-changes 68029-68030
```

```
% fnext
```

```
pkgsrc-wip-changes 10349
```

¹¹From `fnext(1)`

Subset of nmh commands: unseen

*«In unseen mode, new executes scan sequences for each matching folder.»*¹²

```
new [-help] [-version] [sequences] [-mode mode] [-folders foldersfile]
```

```
fnext is equivalent to new -mode fnext
```

```
fprev is equivalent to new -mode fprev
```

```
unseen is equivalent to new -mode unseen
```

```
% unseen
```

```
1 unseen messages in netbsd-source-changes
```

```
N 40500 Kamil Rytarowski Fri Jun 29 11:33 CVS commit: src
```

```
2 unseen messages in pkgsrc-changes
```

```
N 68029 Jonathan Perkin Fri Jun 29 11:27 CVS commit: pkgsrc/pkgtools/pkgin
```

```
N 68030 Jonathan Perkin Fri Jun 29 11:28 CVS commit: pkgsrc/doc
```

```
1 unseen messages in pkgsrc-wip-changes
```

```
N 10349 Havard Eidnes Tue Jun 26 22:42 Do away with use of pip in setup.py.
```

¹²From unseen(1)

Subset of nmh commands: pick

«pick searches within a folder for messages with the specified contents, and then identifies those messages. Two types of search primitives are available: pattern matching and date constraint operations.»¹³

```
pick [-help] [-version] [+folder] [msgs] [-reverse ...] [-and ...] [-or ...] [-not ...] [-lbrace ... -rbrace] [--component pattern] [-cc pattern] [-date pattern] [-from pattern] [-search pattern] [-subject pattern] [-to pattern] [-after date] [-before date] [-datefield field] [-sequence name ...] [-nosequence] [-public | -npublic] [-zero | -nozero] [-list | -nolist] [-debug]
```

```
% pick -search 'CVE-' +pkgsrc-changes last:150
67887
67990
67992
68015
68019
```

```
% scan 'pick -search 'CVE-' +pkgsrc-changes last:150'
N 67887 Thomas Klausner    Sun Jun 24 10:16 CVS commit: pkgsrc/graphics/GraphicsMagick
N 67990 Maya Rashish       Tue Jun 26 21:49 CVS commit: pkgsrc/www/firefox52
N 67992 Maya Rashish       Tue Jun 26 23:29 CVS commit: pkgsrc/www/seamonkey
N 68015 Ryo ONODERA        Thu Jun 28 13:52 CVS commit: pkgsrc/www/firefox
N 68019 Ryo ONODERA        Thu Jun 28 14:04 CVS commit: pkgsrc/www/firefox60
```

¹³From pick(1)

Subset of nmh commands: mark

«*The mark command manipulates message sequences by adding or deleting message numbers from folder-specific message sequences, or by listing those sequences and messages.*»¹⁴

```
mark [-help] [-version] [+folder] [msgs] [-sequence name ...] [-add |
-delete] [-list] [-public | -npublic] [-zero | -nozero]
```

```
% scan 'pick -from maya -and -search 'CVE-' +pkgsrc-changes last:150'
```

```
N 67990 Maya Rashish      Tue Jun 26 21:49 CVS commit: pkgsrc/www/firefox52
N 67992 Maya Rashish      Tue Jun 26 23:29 CVS commit: pkgsrc/www/seamonkey
```

```
% mark -sequence needspullup 'pick -from maya -and -search 'CVE-' +pkgsrc-changes last:150'
```

```
% scan needspullup
```

```
N 67990 Maya Rashish      Tue Jun 26 21:49 CVS commit: pkgsrc/www/firefox52
N 67992 Maya Rashish      Tue Jun 26 23:29 CVS commit: pkgsrc/www/seamonkey
```

¹⁴From mark(1)

pkgsrc Security Team tasks and workflow

Mission

The mission of pkgsrc Security Team is:

- ▶ ensure that packages in pkgsrc are safe
- ▶ be sure pkgsrc users are aware of the known vulnerabilities

Who?

Current members of `pkgsrc-security@` are:

- ▶ Alistair G. Crooks (`<agc>`)
- ▶ Daniel Horecki (`<morrr>`)
- ▶ Thomas Klausner (`<wiz>`)
- ▶ Tobias Nygren (`<tnn>`)
- ▶ Ryo ONODERA (`<ryoon>`)
- ▶ Fredrik Pettai (`<pettai>`)
- ▶ Jörg Sonnenberger (`<joerg>`)
- ▶ Leonardo Taccari (`<leot>`)
- ▶ Tim Zingelman (`<tez>`)

pkgsrc-security@ rotation list

Daniel Horecki <morrr>, Tobias Nygren <tnn>, Ryo ONODERA <ryoon> and Leonardo Taccari <leot> are in the pkgsrc-security@ rotation list.

- ▶ Each person is 'on' from Tuesday till Monday (once every 4 weeks)
- ▶ Ensure that all tickets get handled ASAP
 - ▶ reject the ones not affecting pkgsrc
 - ▶ add entries to pkg-vulnerabilities
 - ▶ inform the MAINTAINER (if any)

RT tickets and the pkgsrc-security queue

- ▶ Each vulnerability is handled via RT (Request Tracker) ticketing system
- ▶ Public security feeds/MLs (e.g. NIST for CVEs) create new tickets on RT
- ▶ Every new ticket and/or RT comments are also received by `pkgsrc-security@` (as emails)

RT ticket statuses used by pkgsrc-security@

- `new` new (usually unhandled) ticket
- `rejected` duplicate issues and ones that do not apply to pkgsrc
- `resolved` ticket that impacts pkgsrc and entry added to `pkg-vulnerabilities`

Handling new tickets

- ▶ Is the ticket a duplicate?
 - ▶ Mark its status as 'rejected'
 - ▶ Add a 'duplicate' comment
- ▶ Does the ticket **not** apply to pkgsrc?
 - ▶ Mark its status as 'rejected' and
 - ▶ Add a 'No impact on pkgsrc' comment.
- ▶ Does the ticket apply to pkgsrc?
 - ▶ Add an entry to pkg-vulnerabilities
 - ▶ Mark its status as 'resolved'
 - ▶ Contact MAINTAINER (if any)

RT tickets (web interface)

RT for NetBSD.org

Logged in as leot | Preferences | Logout

Found 107 tickets

New Search · Edit Search · Advanced · Show Results · Bulk Update · Graph

Home
Simple Search
Tickets
Tools
Preferences
Approval

New ticket in pkgsrc-secur search...

Spreadsheet · RSS · iCal · Editable text

#	Subject	Status	Queue	Owner	Priority
	Requestors	Created	Told	Last Updated	Time Left
127145	CVE-2017-17688 (airmail, emclient, horde_imp, mail, mailldroid, mailmate, outlook, postbox, r2mail2, thunderbird, webmail) rs@netbsd.org	new 5 days ago	pkgsrc-security	Nobody	50 5 days ago
127146	CVE-2017-17689 (airmail, emclient, evolution, gmail, horde_imp, kmail, mail, mailldroid, mailmate, nine, notes, outlook, postbox, r2mail2, the_bat, thunderbird, trojita) rs@netbsd.org	new 5 days ago	pkgsrc-security	Nobody	50 5 days ago
127427	CVE-2016-10525 (hapi-auth-jwt2) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127428	CVE-2014-10066 (fancy-server) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127429	CVE-2015-8094 (hue) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127430	CVE-2015-9244 (mysql_node_module) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127431	CVE-2017-16047 (mysq[ls]) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127432	CVE-2017-16046 (mariadb) rs@netbsd.org	new 27 min ago	pkgsrc-security	Nobody	50 27 min ago
127433	CVE-2017-16058 (gruntcli) rs@netbsd.org	new	pkgsrc-security	Nobody	50

< All

Screenshot of new RT tickets for the pkgsrc-security queue

RT ticket #127438 – CVE-2017-16068

The screenshot displays an RT ticket interface. On the left is a navigation sidebar with options like 'Advanced', 'Show Results', and 'Bulk Update'. The main content area is divided into sections: 'The Basics' (ID: 127438, State: new, Priority: 50), 'Custom Fields' (state: (no value), CERT VULN: (no value), CVE ID: CVE-2017-16068), 'Reminders', 'Dates', 'Links', 'People', and 'More about National Vulnerability Database'. Below this is the 'History' section, showing a message from the National Vulnerability Database dated Mon Jul 02 20:18:26 2018. The message text describes a malicious module named 'fmepegg' and includes links to the NVD entry and a web page. A 'Download' button is visible next to the message content.

Advanced
Show Results
Bulk Update
Graph
<< First
< Prev
#127438
Next >
Last >>
Tools
Preferences
Approval

The Basics
Id: 127438
State: new
Priority: 50
Queue: pkgsrc-security

Custom Fields
state: (no value)
CERT VULN: (no value)
CVE ID: CVE-2017-16068

Reminders
Dates
Links
People
More about National Vulnerability Database

History
Mon Jul 02 20:18:26 2018 **National Vulnerability Database - Ticket created**
To: "pkgsrc-security" <pkgsrc-security-lists@NetBSD.org>
Subject: CVE-2017-16068 (fmepegg)
Date: Mon, 02 Jul 2018 22:18:04 +0000
From: "National Vulnerability Database" <rss@mvd.nist.gov>

fmepegg was a malicious module published with the intent to hijack environment variables. It has been unpublished by npm.

Home: [<http://mvd.nist.gov/>]
Link: [<https://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2017-16068>]

Download (untitled) / with headers
text/plain 225b

Screenshot of RT ticket #127438, CVE-2017-16068

Updating multiple tickets on RT

127531 CVE-2018-9276
rs@red.nist.gov

new pkgsrc-security Nobody 50
30 min ago 30 min ago

Check All Clear All Update

Update multiple tickets

Make Owner: (Force change) Make subject:
Add Requestor: Make priority:
Remove Requestor: Make queue:
Add Cc: Make Status:
Remove Cc: Make date Starts: Calendar
Add AdminCc: Make date Started: Calendar
Remove AdminCc: Make date Told: Calendar
Make date Due: Calendar
Make date Resolved: Calendar

Add comments or replies to selected tickets

Update Type: Comments (not sent to requestors)
Subject:
Attach: No file selected.
 No impact on pkgsrc
Message:

< 80%

Screenshot of updating multiple tickets on RT

pkg_admin(1) and vulnerabilities

pkg_admin(1) has several commands to inform users about vulnerable packages installed on system.

`audit` print a list of all installed packages that contain vulnerabilities On NetBSD, if the `check_pkg_vulnerabilities` option is set (it is by default ¹⁵) the `daily(5)` cron job will list all vulnerability packages installed.

`fetch-pkg-vulnerabilities` fetch a new `pkg-vulnerabilities` file ¹⁶. This is disabled by default and can be configured via `daily.conf(5)` by adding `fetch_pkg_vulnerabilities=YES` in `/etc/daily.conf`.

¹⁵Please give a look to `security.conf(5)` if you are curious!

¹⁶By default it is downloaded from `ftp.NetBSD.org`

pkg_admin audit in action

```
% pkg_admin audit
Package pcre-8.42 has a denial-of-service vulnerability, see
  https://nvd.nist.gov/vuln/detail/CVE-2017-11164
Package libxslt-1.1.32 has a insufficiently-random-numbers vulnerability, see
  https://nvd.nist.gov/vuln/detail/CVE-2015-9019
Package jpeg-9c has a denial-of-service vulnerability, see
  https://nvd.nist.gov/vuln/detail/CVE-2018-11813
[...]
```

pkg-vulnerabilities

pkg-vulnerabilities is a TSV ¹⁷ that contains 3-uples:

`package` PKGNAME patterns ¹⁸

`type of exploit` (e.g. denial-of-service, buffer-overflow, multiple-vulnerabilities, eol, ...)

`URL` URL that contains details about the vulnerability (often to `nvd.nist.gov` for CVEs)

¹⁷Actually `[\t]SV!`, i.e. `awk '! /^#/ { print $1, $2, $3 }'` will DTRT!

¹⁸In case of doubt you can use `pkg_admin pmatch pattern pkg` that returns true if 'pkg' matches 'pattern', e.g. `pkg_admin pmatch 'foo<1.0' 'foo-1.0'` will return false.

Some numbers

Tickets handled in 2016	
Status	Tickets
rejected	10429
resolved	1367
stalled	0
Total	11796

Tickets handled in 2017	
Status	Tickets
rejected	23511
resolved	2847
stalled	2
Total	26360

- ▶ Number of vulnerable packages in pkgsrc head: 591 ¹⁹
- ▶ Number of vulnerable packages in pkgsrc stable [2018Q1]: 624 ²⁰

¹⁹As of 2018-07-03 4:00 UTC

²⁰As of 2018-07-03 4:00 UTC

Automating the automatable stuffs of pkgsrc-security

Request Tracker (RT) REST Interface

- ▶ Request Tracker (RT) provides a REST interface that permit to programmatically access RT databases.
- ▶ Both `devel/rt3` and `devel/rt4` provides a `rt` Perl script
- ▶ Other package/modules exists for several programming languages

rt: command-line interface to RT

- ▶ Perl script that can be used both non-interactively (directly passing action when invoking it) or interactively (if no action are passed, i.e. just by invoking it as 'rt')
- ▶ Actions most commonly used:
 - `list` show a list of tickets
 - `show` show information about a ticket (description, updates, comments)
 - `edit` modify fields of a ticket
 - `comment` add a comment to a ticket
 - `help` print help message

rt actions: list

«Displays a list of objects matching the specified conditions. ("ls", "list", and "search" are synonyms.)»²¹

```
rt <ls|list|search> [options] "query string"
```

To show all ticket in the 'new' status:

```
% rt ls -s Status=new
127145: CVE-2017-17688 (airmail, emclient, ...)
127146: CVE-2017-17689 (airmail, emclient, ...)
127451: CVE-2018-0499 (xapian)
127458: CVE-2018-10874 (ansible)
127470: CVE-2018-11489 (giflib, sam2p)
127472: CVE-2018-11490 (giflib, sam2p)
127504: CVE-2018-13033 (binutils)
127511: CVE-2018-13049 (php-glp)
127517: CVE-2018-13066 (ming)
127537: CVE-2017-2615 (qemu)
127539: CVE-2018-10855 (ansible2)
127668: CVE-2018-13100 (linux)
127672: CVE-2018-13112 (tcpdump)
127710: [SECURITY] [DSA 4238-1] exiv2 security update
127735: CVE-2018-3750 (npm)
```

²¹From `rt help list`

rt actions: show

«*Displays details of the specified objects.*»²²

```
rt show [options] <object-ids>
```

To show information about ticket #127668:

```
% rt show 127668
Date: Tue Jul 03 20:19:32 2018
From: rss@nvd.nist.gov
X-Queue: pkgsrc-security
Subject: [rt #ticket/127668] CVE-2018-13100 (linux)

==> Ticket created by rss@nvd.nist.gov on Tue Jul  3 22:19:33 2018
An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3,
which does not properly validate secs_per_zone in a corrupted f2fs image, as
demonstrated by a divide-by-zero error.

Home: [http://nvd.nist.gov/]
Link: [ https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-13100 ]
      544638: untitled (300b)
==> Outgoing email recorded by RT_System on Tue Jul  3 22:19:33 2018
      544640: untitled (606b)
==> CVE IDs CVE-2018-13100 added by leot on Wed Jul  4 11:21:08 2018
==> Subject changed from 'CVE-2018-13100' to 'CVE-2018-13100 (linux)'
      by leot on Wed Jul  4 12:05:33 2018
```

²²From `rt help show`

rt actions: edit

«Edits information corresponding to the specified objects.»²³

```
rt edit [options] <object-ids> set field=value [field=value] ...
                                add field=value [field=value] ...
                                del field=value [field=value] ...
```

Ticket #127668 (CVE-2018-13100) does not affect pkgsrc so we can close it:

```
% rt edit 127668 set status=rejected
# Ticket 127668 updated.
```

²³From `rt help edit`

rt actions: comment

«Adds a comment (or correspondence) to the specified ticket (the only difference being that comments aren't sent to the requestors.)»²⁴

```
rt <comment|correspond> [options] <ticket-id>
```

#127668 had no impact on pkgsrc, so let's add a comment about that:

```
% rt comment -m 'No impact on pkgsrc' 127668  
# Message recorded
```

²⁴From `rt help comment`

Automating tickets handling from the MUA (or, putting everything together!)

- ▶ All (new) RT tickets and comments ends up in an MH folder
- ▶ The CVE ones from NIST have a CVE- [0-9]+- [0-9]+ pattern in the Subject:, we can automatically fill the CVE IDs field to RT
- ▶ All the ones that have no impact on pkgsrc can be marked with a special sequence (e.g. 'marked') and then automatically marked as 'rejected' with a 'No impact on pkgsrc' comment
- ▶ Usually when receiving CVE tickets no information about the package is present in the Subject:, they can be marked with a PKGBASE sequence (e.g. 'qemu') and then update the subject of the ticket accordingly to ease further processing when filling respective pkg-vulnerabilities entries

Automating tickets handling from the MUA (or, putting everything together!)

- ▶ Duplicate CVE tickets that are already in `pkg-vulnerabilities` can be automatically rejected by parsing `rt ls Status=new` output and URL field of `pkg-vulnerabilities` matching the `CVE-[0-9]+-[0-9]+` patterns
- ▶ Duplicate tickets in the `pkgsrc-security` queue can be easily rejected similarly
- ▶ After marking CVE tickets as described an entry for `pkg-vulnerabilities` can be populated with a template, e.g.:

```
PKGBASE-[0-9]+ TODO https://nvd.nist.gov/vuln/detail/CVE-<id>
```

Filling CVE IDs in the ticket

Instead of doing that in shell scripting and `rt`, it is easier to use `wip/py-rt`:

```
import rt

tracker = rt.Rt(RT_API_URL, basic_auth=(username, password))
tracker.login()

for ticket in tracker.search(Queue='pkgsrc-security', Status='new',
                             Subject__like='CVE', Format='s'):
    cves = re.findall('CVE-[0-9]+-[0-9]+', ticket['Subject'])
    if cves:
        fields = { 'CF_CVE IDs': ' '.join(cves) }
        tracker.edit_ticket(ticket['id'].replace('ticket/', ''), **fields)
```

Closing marked tickets

```
% scan +pkgsrc-security-rt marked
N 81635 National Vulnerab Wed Jul 04 20:18 [NetBSD.org #127747] CVE-2018-13144
[...]
>N 81641 National Vulnerab Wed Jul 04 20:18 [NetBSD.org #127753] CVE-2018-13145

% scan -format '%{rt-ticket}' +pkgsrc-security-rt marked
NetBSD.org #127747
[...]
NetBSD.org #127753

% scan -format '%{rt-ticket}' +pkgsrc-security-rt marked | cut -d '#' -f 2
127747
[...]
127753

% scan -format '%{rt-ticket}' +pkgsrc-security-rt marked |
  cut -d '#' -f 2 | xargs rt edit set status=rejected
# Ticket 127747 updated.
[...]
# Ticket 127753 updated.

% scan -format '%{rt-ticket}' +pkgsrc-security-rt marked |
  cut -d '#' -f 2 | xargs -n 1 rt comment -m 'No impact on pkgsrc'
# Message recorded
[...]
# Message recorded
```

Report all 'new' CVE duplicate tickets

The format of `rt ls -s` is²⁵:

`<id>: <subject>`

```
rt ls -s |
awk \
{
    # Get rid of ':' in the ticket id
    sub(/:$/, "", $1)
}
$2 ~ /CVE-[0-9]+-[0-9]+/ {
    id = $1
    cve = $2

    if (cves[cve])
        print id
    else
        cves[cve] = id
}
,
```

²⁵E.g.: 127750: CVE-2018-13139

Report all CVE tickets that are already in pkg-vulnerabilities

```
(cat $pkgvulnerabilities ; rt ls -s ) | awk \
,
# Slurp pkg-vulnerabilities CVE entries in vuln[]
$3 ~ /CVE-[0-9]+-[0-9]+/ {
    pkgname = $1
    type = $2
    match($3, /CVE-[0-9]+-[0-9]+/)
    cve = substr($3, RSTART, RLENGTH)

    entry[cve] = $0

    next
}

# Parse rt ls -s output
$2 ~ /CVE-[0-9]+-[0-9]+/ {
    id = $1
    match($2, /CVE-[0-9]+-[0-9]+/)
    cve = substr($2, RSTART, RLENGTH)

    if (entry[cve]) {
        print id " " entry[cve]
    }
}
,
```

Conclusion

- ▶ Reading/skimming tickets needs humans...
- ▶ ...but at least when handling a lot of tickets scripting can ease a lot!

Thanks

- ▶ pkgsrc Security Team and everyone who help keeping up to date pkg-vulnerabilities and requests pullups!
- ▶ pkgsrc Releng for their work!

References I

Robert H. Anderson, Norman Shapiro, Tora K. Bikson, Phyllis Kantar.

The Design of the MH Mail System.

<https://www.rand.org/pubs/notes/N3017.html>.

Request Tracker Wiki.

REST - Request Tracker Wiki.

<https://rt-wiki.bestpractical.com/wiki/REST>.

Alistair Crooks, Hubert Feyrer, The pkgsrc Developers.

The pkgsrc guide.

<https://www.NetBSD.org/docs/pkgsrc/>.

References II

Thomas A. Limoncelli.

Manual work is a bug.

Queue, 16(1):20:13–20:29, February 2018.

ISSN 1542-7730.

doi: 10.1145/3194653.3197520.

URL <http://doi.acm.org/10.1145/3194653.3197520>.

Questions?