Development and maintenance of Suricata

OISF

SURICATA

November 9-11, 2022

About me

- Developing parts of [Suricata, all the helper tools]

@tuxish

@inashivb

shivanibhardwaj.com

SURICON ATHENS 2022

How do we maintain a stable release

1. Instant reviews (almost) of every ticket for master especially bug fixes/security issues
2. Labeling the tickets to backport to the stable version
3. Fixup in master
4. Backport the fix to stable branch
5. Testing

SURICON ATHENS 2022

Effort that goes in the making of a stable release

SURICON ATHENS 2022

Reviews

For bugs:
Requires manual testing if the issue exists in the stable branch

For features/optimizations:
Requires checking if it could lead to a behavior change

SURICON ATHENS 2022

Labeling

1. Manual labeling of the tickets

Fix and backporting

1. Making sure the fix in master works
2. Backporting after the merge to establish a clear relationship

SURICON ATHENS 2022

Bug #4274 CLOSED

Suricata crashes at exit in NFQ mode

Added by Eric Leblond almost 2 years ago. Updated over 1 year ago.

Status:	Closed		
Priority:	Normal		
Assignee:	Eric Leblond		
Target version:	7.0.0-beta1		
Affected Versions:		**Difficulty:**	
Effort:	low	**Label:**	Needs backport to 5.0, Needs backport to 6.0

SURICON ATHENS 2022

Development and maintenance of a stable branch

SURICON ATHENS 2022

Rev 1

Issue tracking (Redmine)

- Tickets were labelled manually
- A copy of the main ticket was created for the target stable branch

On the stable branch

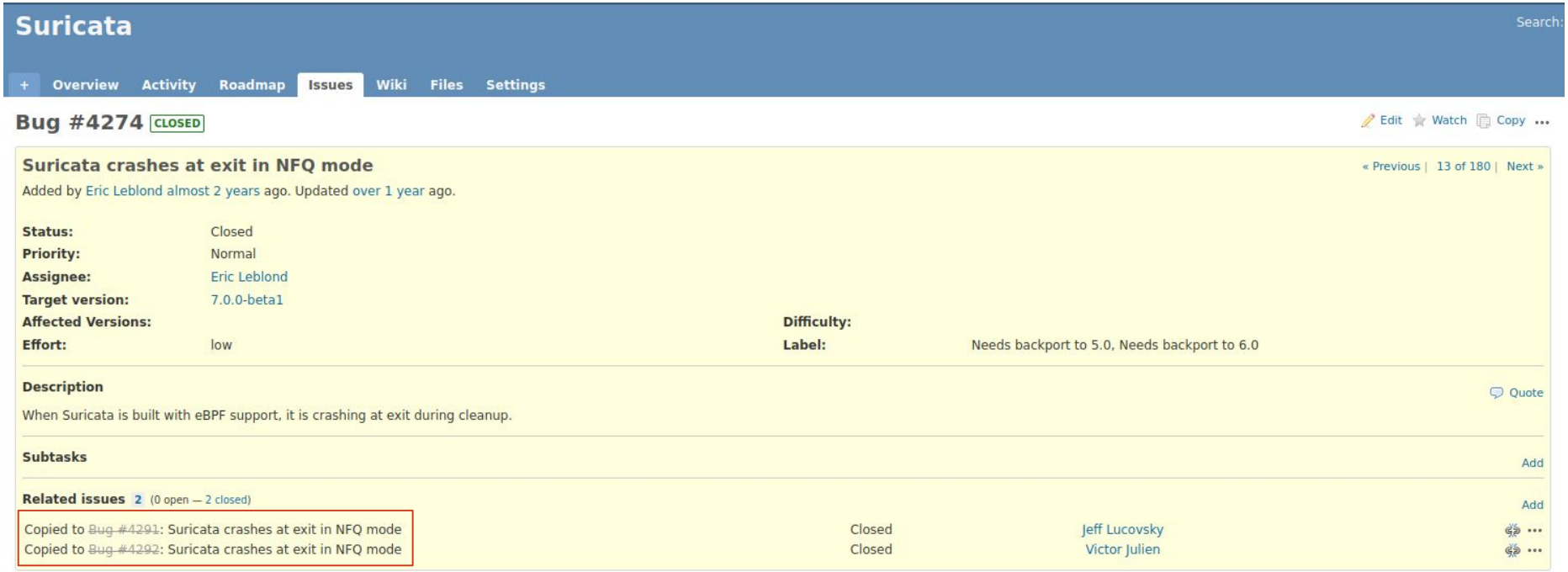
- Fixes were cherry-picked

SURICON ATHENS 2022

Cons - rev 1

1. Missed creation of backport tickets
2. Updated info in parent ticket
3. Unclear cherry-picks of one or more relevant commits especially if they required modification

SURICON ATHENS 2022



SURICON ATHENS 2022

Improvise

SURICON ATHENS 2022

Rev 2

SURICON ATHENS 2022

Cons - rev 1

1. Missed creation of backport tickets
2. Unclear cherry-picks of one or more relevant commits

→ Create subtickets instead of copies to make sure the main ticket doesn't get closed up until the fix has already been backported.

→ Commit hashes of the main commit mandatorily a part of the backported commits for easy tracking.

SURICON ATHENS 2022

Bug #5395 CLOSED

~~Bug #5208~~: DCERPC protocol detection when nested in SMB

DCERPC protocol detection when nested in SMB (6.0.x backport)

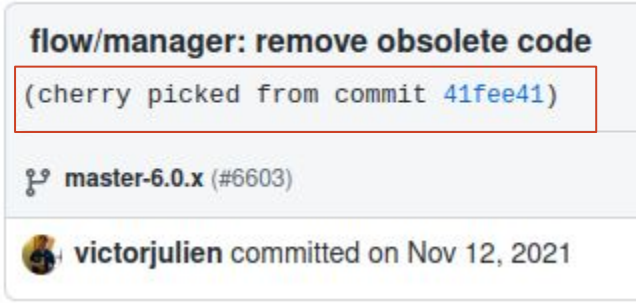
Added by Victor Julien 5 months ago. Updated 5 months ago.

Status:	Closed
Priority:	Normal
Assignee:	Victor Julien
Target version:	6.0.6
Affected Versions:	
Effort:	

Subtasks

Related issues

SURICON ATHENS 2022



SURICON ATHENS 2022

Cons - rev 2

1. Accidental missing/incorrect commit hashes in the backported commits
2. No reliable correlation with the tickets yet.

SURICON ATHENS 2022

Improvise

SURICON ATHENS 2022

Cons - rev 2

1. Accidental missing/incorrect commit hashes in the backported commits
2. No reliable correlation with the tickets yet.

→ CI checks for missing/incorrect commit hashes

→ Mandatory to add Redmine ticket in the commit message

SURICON ATHENS 2022

victorjulien github-ci: add cherry-pick line check ✕ Latest commit 275975c on Sep 5 **History**

1 contributor

Executable File | 40 lines (33 sloc) | 976 Bytes Raw Blame

```
#!/bin/bash

#set -x
#set -e

if [ $# -ne 1 ]; then
    echo "call with base branch (e.g. master-5.0.x)"
    exit 1;
fi

BASE=$1
CHECK_BRANCH="${VALIDATE_CHECK_BRANCH:-remotes/origin/master}"

test_cherrypicked_line() {
    REV=$1
    #echo "\"REV $REV\""

    CHERRY=$(echo $REV | grep '(cherry picked from commit' | awk '{print $5}'|awk -F')' '{print $1}' || return 1)
    git branch -a --contains $CHERRY | grep " $CHECK_BRANCH$" &> /dev/null
    if [ "$?" -ne 0 ]; then
        echo -n "ERROR $CHERRY not found in $CHECK_BRANCH"
        return 1
    else
        echo -n "OK "
    fi
```

SURICON ATHENS 2022

Why is it important to stay up-to-date with the latest stable Suricata

SURICON ATHENS 2022

Fuzzing

Other (non)security issues

SURICON ATHENS 2022

Cost of maintaining 2 stable branches

SURICON ATHENS 2022

A lot higher than double. Why?

1. Usually the older branch is too behind master
2. All fixes in master cannot be backported as they are or with small tweaks
3. New patches need to be written for certain fixes from scratch

SURICON ATHENS 2022

Automation effort

Ticket creation/checking

- Tickets are automagically created for backporting – More reliable
- Tickets are auto checked and dev informed if a branch is ready for the release i.e. all relevant tickets are closed.

SURICON ATHENS 2022

Release: Three stages

1. **Prep**: All the preparation and checks of tickets and commits. Staging branch -> Release branch
2. **Push**: Pushing the prepared and manually verified release tarball to all the relevant places. Publishing the Release branch
3. **Announce**: Preparation and posting of release on Twitter, Discourse.

SURICON ATHENS 2022

Aim

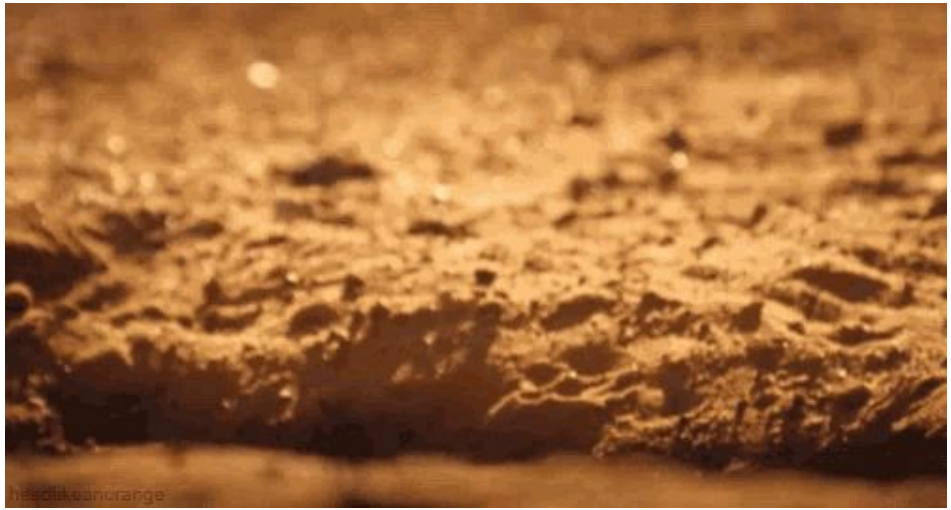
More automation and testing that can enable
Timely scheduled Suricata releases (stable)

SURICON ATHENS 2022

Conclusion

- Lots of (not very obvious) effort happening around maintenance and shipping of releases
- A little extra effort happening right now in automation to cut down manual effort and make the process easier and reliable

SURICON ATHENS 2022



Questions?

SURICON ATHENS 2022