

NixOS Security

Vulnerability Roundup n + 1

Graham Christensen

Vulnerability Roundup 0

2016-02-27

<fpletz> gchristensen: yeah, just wanted to do a quick security survey because we will branch off for the next release today :)

what is lwn?

- Linux newspaper
- Tracked vulnerabilities
 - collected security disclosures
 - aggregated across distros

```
commit ed6ea7416aafdf96aa6cc87e165569bb79c42be0
Author: Domen Kozar <domen@dev.si>
Date:   Sun Aug 28 19:59:08 2016 +0200
```

Document NixOS release process #4442

```
--- /dev/null
+++ b/nixos/doc/manual/development/releases.xml
```

```
+     <listitem>
+         <para>
+             Use https://lwn.net/Vulnerabilities/ and
+             triage vulnerabilities in an issue.
+         </para>
+     </listitem>
```

Vulnerability Roundup 1

- [] [#699805](#) ([search](#), [files](#)) 389-ds-base: information disclosure
- [] [#675820](#) ([search](#), [files](#)) 389-ds-base: denial of service



845 items not shown

[View more](#)

- [] [#687229](#) ([search](#), [files](#)) xerces-c: code execution
- [] [#677608](#) ([search](#), [files](#)) xerces-c: code execution

authors

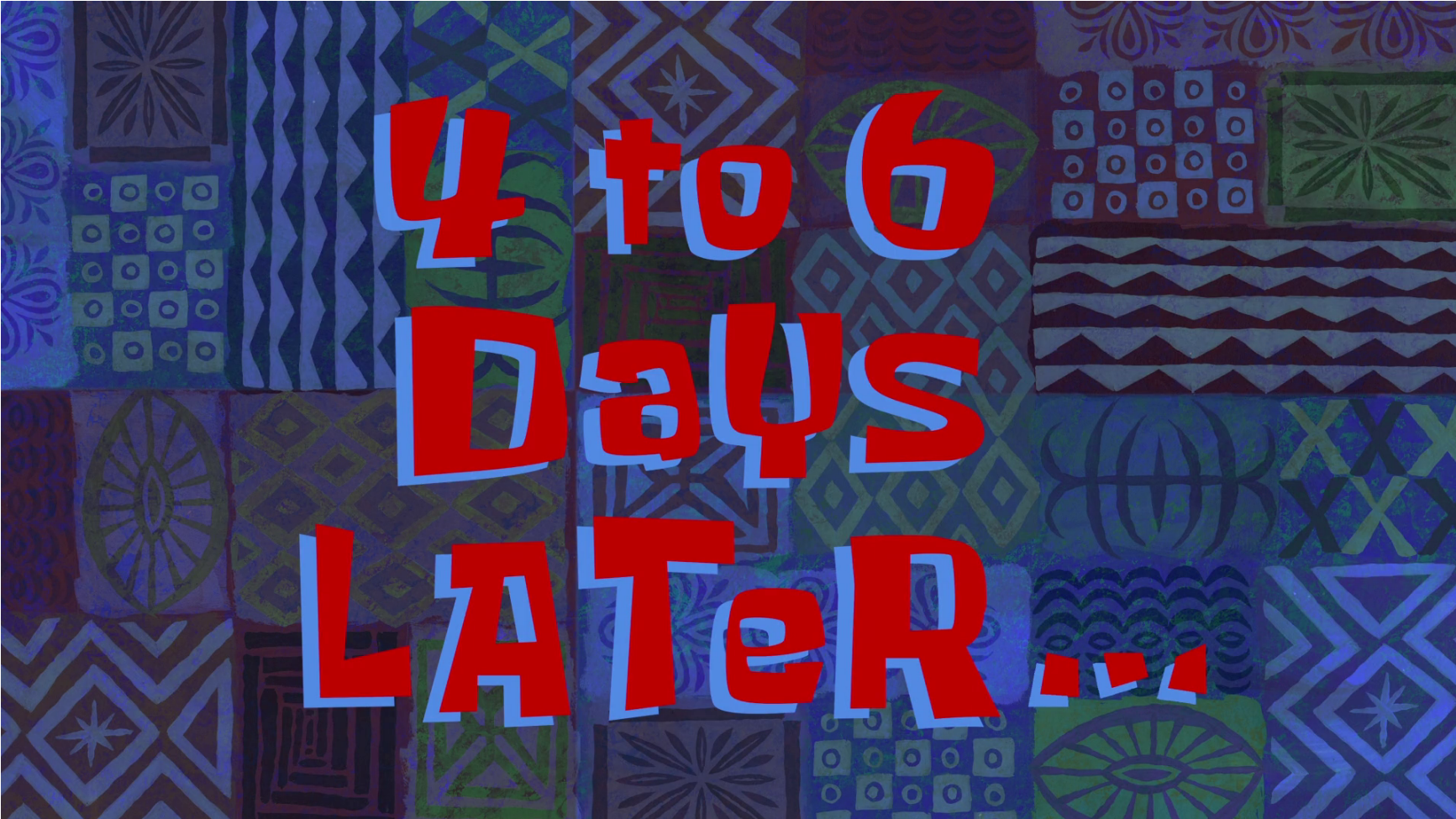
- @fpletz
- @aneeshusa
- @jagajaga
- @joachifm
- @Mic92
- @NeQuissimus
- @RamKromberg
- @schneefux
- @vrtha

reviewers

- @7c6f434c
- @HappyEnte
- @kevincox

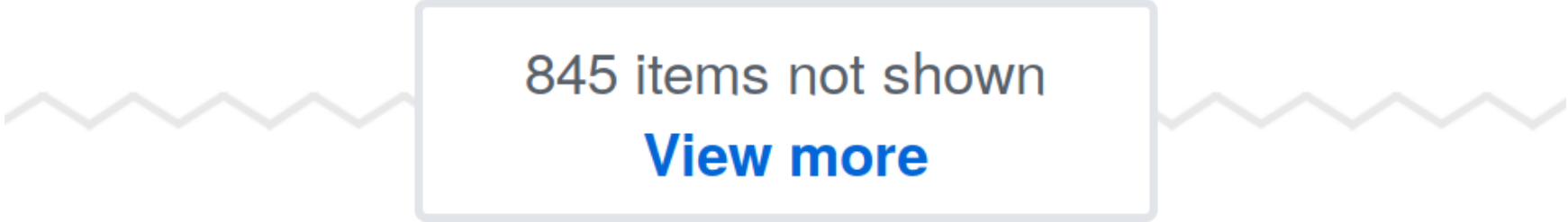
mergers

- @bjornfor
- @DamienCassou
- @edolstra
- @svanderburg
- @vcunat
- @zimbatm



**4 to 6
Days
Later...**

- [X] [#699805](#) ([search](#), [files](#)) 389-ds-base: information disclosure
- [X] [#675820](#) ([search](#), [files](#)) 389-ds-base: denial of service



845 items not shown
[View more](#)

- [X] [#687229](#) ([search](#), [files](#)) xerces-c: code execution
- [X] [#677608](#) ([search](#), [files](#)) xerces-c: code execution

16.09 was really good.

prompt, regular security patching
a community effort

Thu Nov 24, 2016

[Nix-dev] Announcing: nix-security-announce Mailing List

Wed Dec 7, 2016

[Nix-dev] NixOS Security Team



**TWELVE
SECONDS LATER**

March 1, 2017

24 Vulnerability Roundups

~ 1,500 triaged reports

```
commit de31f879bd1a08ed35f9e3b632a5ab22837b58be
Author: Robin Gloster <mail@glob.in>
Date:   Wed Aug 30 22:23:56 2017 +0200
```

release documentation: update to current procedure

```
--- a/nixos/doc/manual/development/releases.xml
+++ b/nixos/doc/manual/development/releases.xml
```

```
-     <listitem>
-         <para>
-             Use https://lwn.net/Vulnerabilities/ and
-             triage vulnerabilities in an issue
-         </para>
-     </listitem>
```



that was then

what's next?

(a personal goal)

Goal: General Commercial Viability

- why: I don't want to go back to puppet

(a personal goal)

Goal: General Commercial Viability

- Nix is predictable and commercial users value this
- ***Safe rollbacks are ENORMOUSLY VALUABLE***
 - Shipping industry: \$1M / deploy

how

demonstrate a commitment to security

- Keep users safe
- Demonstrate we won't abandon the project

option

Watch all CVEs?

better option

Watch oss-security?

goal

distros@vs.openwall.org

- Lead time on embargoed security patches

requirements

Be an actively maintained Unix-like operating system distro with substantial use of Open Source components

requirements

Have a userbase not limited to your own organization

requirements

**Not be downstream or a rebuild of
another distro**

requirements

Have someone already on the private list vouch for people requesting membership

maybe peti can help :)

requirements

Have a track record of at least 1 year of fixing security issues

...

within 10 days

the major blocking issue

Consistency

the hard thing about consistency

**We can't choose to be consistent, here,
today**

**We must wake up every day and
choose to be consistent**

Make NixOS Really Good 1

[Edit](#)



Do a security round up

10/25/17, 13:00, Weekly

Consistency

- most distros triage oss-security reports by hand
- need tools or processes to ensure good coverage
- we must share the load to prevent burnout

how to help

- monitor oss-security for announcements
- hear of a bug? send a patch NixOS
- can't patch? open an issue

how to help, continued

try stuff

yes, you :)

easier blocking issues

- private bug tracker
- private build jobs
- private code branch

not such an issue

build farm speed

| 7 to 10 days

but let's make it better anyway

- Zero Hydra Failures ... forever
- better PR testing and review tools
- ***bonus*** easier to merge

attempt

Hydra PRs



grahamc commented on Jan 26

Member



Everything builds ok according to <https://prs.nix.gsc.io/jobset/nixos/pr-22163>, too. Thank you!

with hardware by

packet

(huge thank you)

attempt

GrahamCOfBorg



GrahamCOfBorg added the **10.rebuild-linux: 1-10** label 23 hours ago

attempt

GrahamCOfBorg



grahamc commented a day ago

Member



@GrahamCOfBorg nnn



GrahamCOfBorg approved these changes a day ago

[View changes](#)

```
cp -f nnn.1 /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/share/man/man1
post-installation fixup
shrinking RPATHs of ELF executables and libraries in /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/bin/nnn
shrinking /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/bin/nnn
zipping man pages under /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/share/man/
stripping (with flags -S) in /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/bin
patching script interpreter paths in /nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5
/nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5/bin/nlay: interpreter directive changed
checking for references to /tmp/nix-build-nnn-1.5.drv-0 in /nix/store/71nhixk6sbk5y4j6v0a0y
/nix/store/71nhixk6sbk5y4j6v0a0ycyg9viq71sg-nnn-1.5
```

surprising bonus news (?)

Common Vulnerabilities and Exposures Numbering Authority

Let's become a CNA

gchristensen on Freenode

github.com/grahamc

twitter.com/grhmc