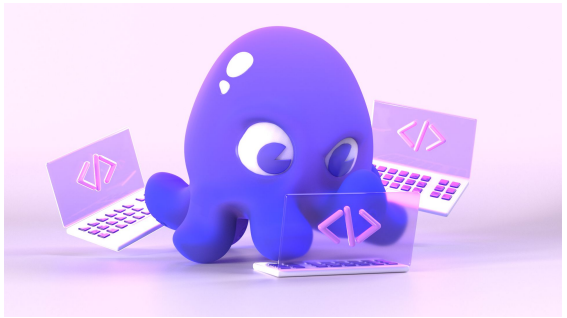
chainguard

12+ Years of Shipping OpenSSL

Dimitri John Ledkov

Hi, I am xnox

- Debian Developer
- Ubuntu Core Developer
- Intel Clear Linux*
- Chainguard



Cryptography contributions

- OpenSSL
- Libressl
- Boringssl
- AWS-LC
- Grub cryptography code
- Kernel crypto API

- Vendor changes to secureboot rhboot/shim “openssl”
- Vendor changes to secureboot edk2 “openssl”

My history with OpenSSL

- Backported ARMv7 hardware-optimisations
- Backported IBM Z / s390x hardware-optimisations
- Upgraded 18.04 LTS from 1.1.0 to 1.1.1
- Raised Security Level to 2 by default
- Disabled TLSv1.1 by default
- Ship latest upstream releases
- Retrofit certified FIPS providers with new OpenSSL

Incompatible “stable” updates

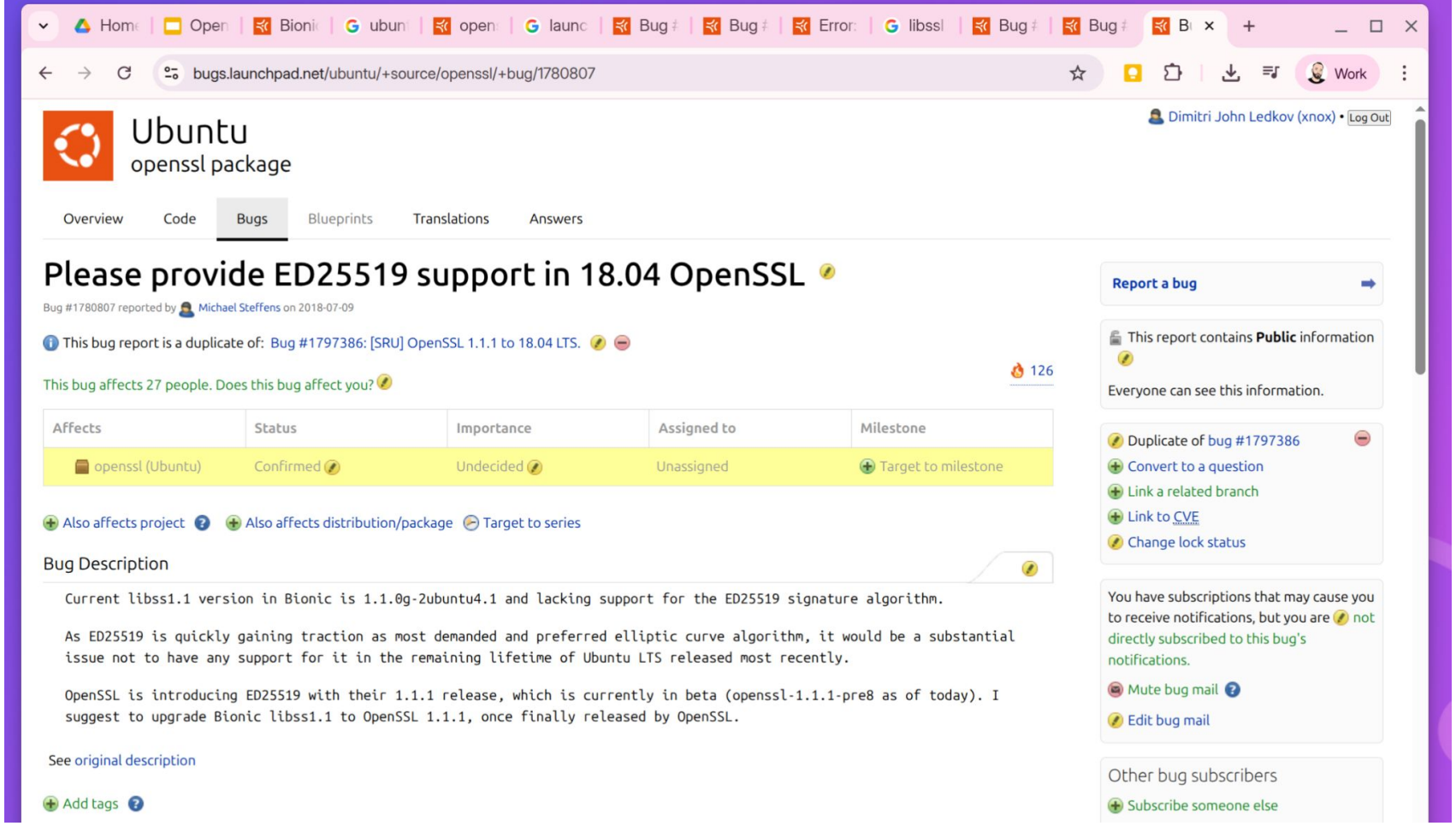
- OpenSSL stable updates policy
- Ubuntu Stable Release Updates

- Ubuntu freezes OpenSSL on a minor point release (1.0.1f, 1.0.2g, 1.1.1f, 3.02, etc)
- Targeted cherry-picks only
- Security fixes, bugfixes, and hardware acceleration
- No ABI changes - because $release-updates is a rolling stream

- OpenSSL stable updates - can change ABI, regression vs feature
- Duplication of work

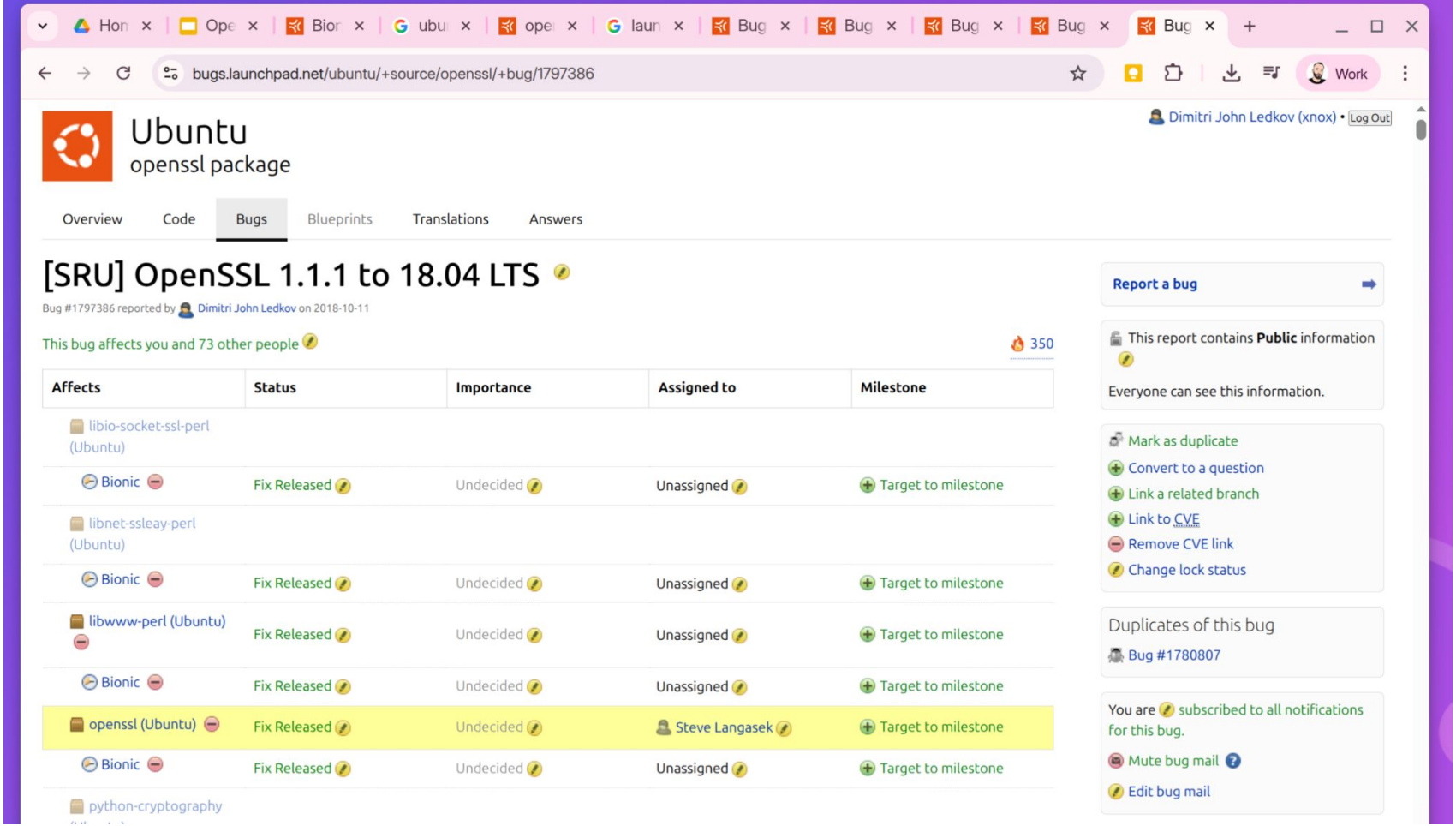
Release Schedules not regular

- Ubuntu 18.04 LTS scheduled for April 2018
- OpenSSL 1.1.1 released September 2018
- With TLSv1.3 support & Ed25519
- Demand anticipated


bugs.launchpad.net/ubuntu/+source/openssl/+bug/1780807
Work
Ubuntu
openssl package
Dimitri John Ledkov (xnox) • Log Out
Overview
Code
Bugs
Blueprints
Translations
Answers
Please provide ED25519 support in 18.04 OpenSSL
Bug #1780807 reported by Michael Steffens on 2018-07-09
This bug report is a duplicate of: Bug #1797386: [SRU] OpenSSL 1.1.1 to 18.04 LTS.
This bug affects 27 people. Does this bug affect you?
126
Affects
Status
Importance
Assigned to
Milestone
openssl (Ubuntu)
Confirmed
Undecided
Unassigned
Target to milestone
Also affects project
Also affects distribution/package
Target to series
Bug Description
Current libss1.1 version in Bionic is 1.1.0g-2ubuntu4.1 and lacking support for the ED25519 signature algorithm.
As ED25519 is quickly gaining traction as most demanded and preferred elliptic curve algorithm, it would be a substantial issue not to have any support for it in the remaining lifetime of Ubuntu LTS released most recently.
OpenSSL is introducing ED25519 with their 1.1.1 release, which is currently in beta (openssl-1.1.1-pre8 as of today). I suggest to upgrade Bionic libss1.1 to OpenSSL 1.1.1, once finally released by OpenSSL.
See original description
Add tags
Report a bug
This report contains Public information
Everyone can see this information.
Duplicate of bug #1797386
Convert to a question
Link a related branch
Link to CVE
Change lock status
You have subscriptions that may cause you to receive notifications, but you are not directly subscribed to this bug's notifications.
Mute bug mail
Edit bug mail
Other bug subscribers
Subscribe someone else

Agreement to backport

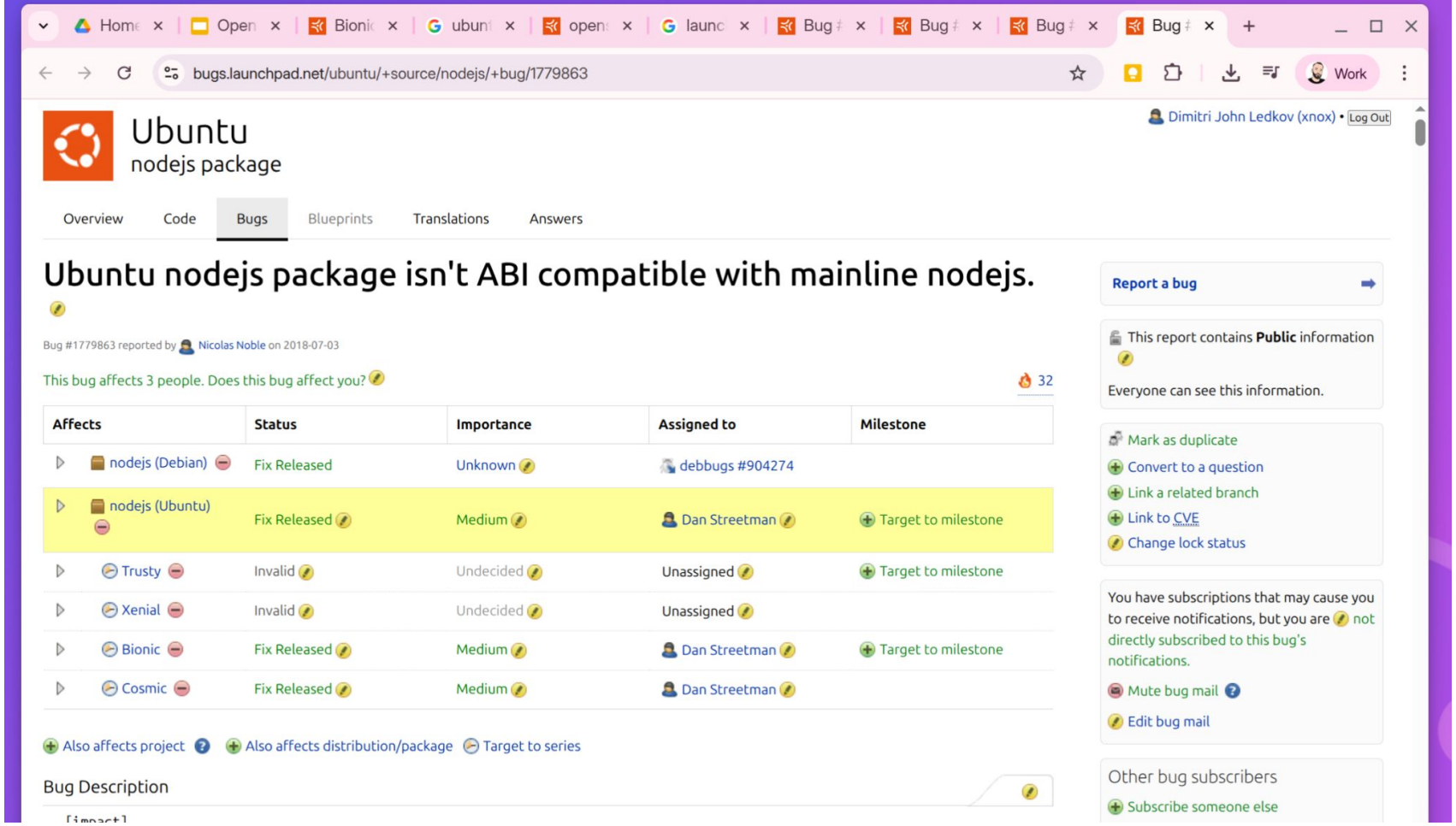
- Agreed to wait for upsteam 1.1.1
- Agreed to backport
- In theory ABI forward compatible
- In theory no changes needed

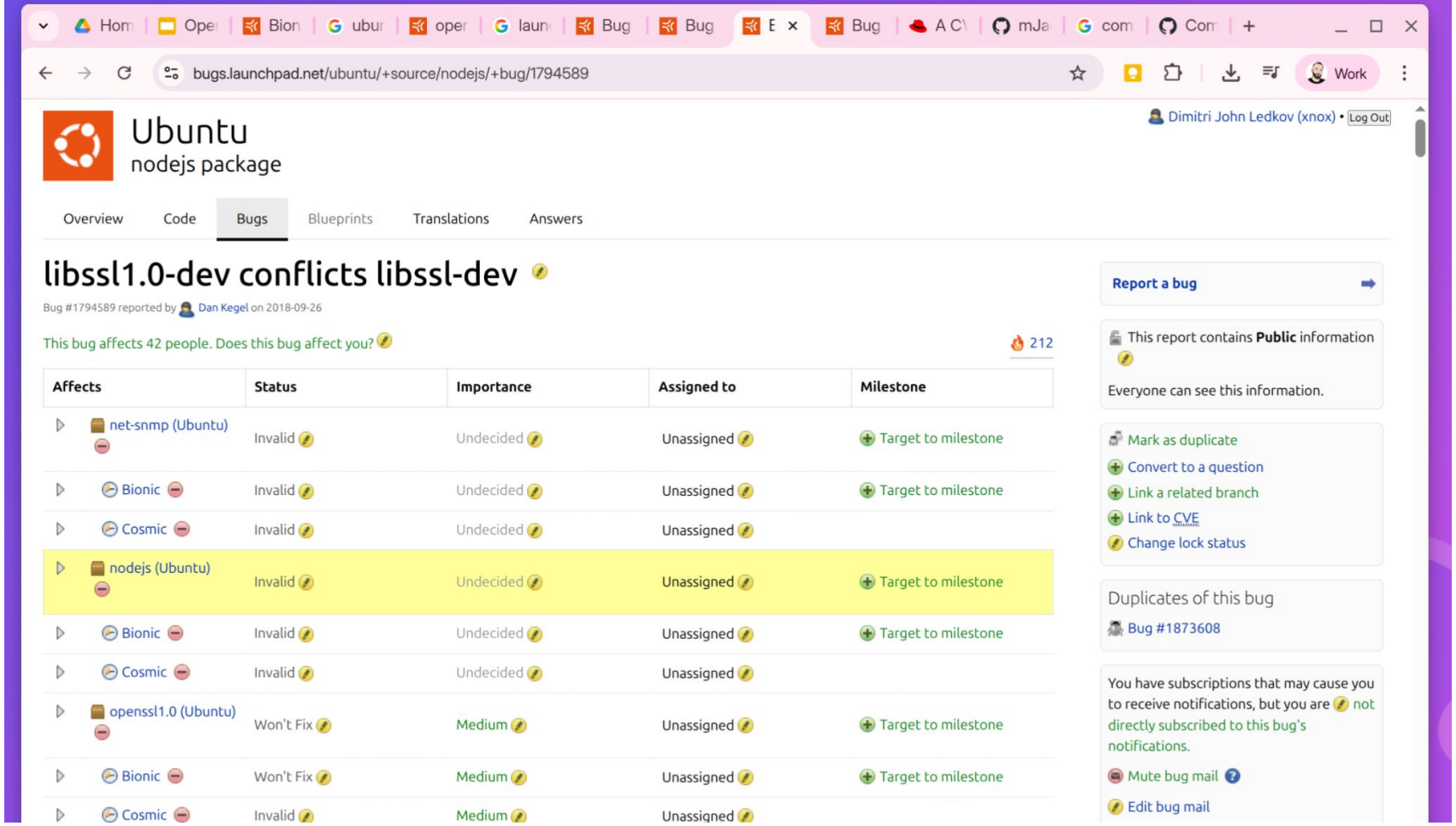

bugs.launchpad.net/ubuntu/+source/openssl/+bug/1797386
Work
Ubuntu
openssl package
Dimitri John Ledkov (xnox) • Log Out
Overview
Code
Bugs
Blueprints
Translations
Answers
[SRU] OpenSSL 1.1.1 to 18.04 LTS
Bug #1797386 reported by Dimitri John Ledkov on 2018-10-11
This bug affects you and 73 other people
350
Affects
Status
Importance
Assigned to
Milestone
libio-socket-ssl-perl (Ubuntu)
Bionic
Fix Released
Undecided
Unassigned
Target to milestone
libnet-ssleay-perl (Ubuntu)
Bionic
Fix Released
Undecided
Unassigned
Target to milestone
libwww-perl (Ubuntu)
Bionic
Fix Released
Undecided
Unassigned
Target to milestone
openssl (Ubuntu)
Fix Released
Undecided
Steve Langasek
Target to milestone
Bionic
Fix Released
Undecided
Unassigned
Target to milestone
python-cryptography
Report a bug
This report contains Public information
Everyone can see this information.
Mark as duplicate
Convert to a question
Link a related branch
Link to CVE
Remove CVE link
Change lock status
Duplicates of this bug
Bug #1780807
You are subscribed to all notifications for this bug.
Mute bug mail
Edit bug mail

Interim result

- ~12+ packages needed upgrades
- Turned out ABI is compatible, but API behaviour changes
- Require code changes to update to new requirements
- Decide to downgrade nodejs to use libssl1.0
- … and that’s it

- Broke nodejs for all


bugs.launchpad.net/ubuntu/+source/nodejs/+bug/1779863
Work
Ubuntu
nodejs package
Dimitri John Ledkov (xnox) • Log Out
Overview
Code
Bugs
Blueprints
Translations
Answers
Ubuntu nodejs package isn't ABI compatible with mainline nodejs.
Bug #1779863 reported by Nicolas Noble on 2018-07-03
This bug affects 3 people. Does this bug affect you?
32
Affects
Status
Importance
Assigned to
Milestone
nodejs (Debian)
Fix Released
Unknown
debbugs #904274
nodejs (Ubuntu)
Fix Released
Medium
Dan Streetman
Target to milestone
Trusty
Invalid
Undecided
Unassigned
Target to milestone
Xenial
Invalid
Undecided
Unassigned
Bionic
Fix Released
Medium
Dan Streetman
Target to milestone
Cosmic
Fix Released
Medium
Dan Streetman
Also affects project
Also affects distribution/package
Target to series
Bug Description
Report a bug
This report contains Public information
Everyone can see this information.
Mark as duplicate
Convert to a question
Link a related branch
Link to CVE
Change lock status
You have subscriptions that may cause you to receive notifications, but you are not directly subscribed to this bug's notifications.
Mute bug mail
Edit bug mail
Other bug subscribers
Subscribe someone else


bugs.launchpad.net/ubuntu/+source/nodejs/+bug/1794589
Work
Ubuntu
nodejs package
Dimitri John Ledkov (xnox) • Log Out
Overview
Code
Bugs
Blueprints
Translations
Answers
libssl1.0-dev conflicts libssl-dev
Bug #1794589 reported by Dan Kegel on 2018-09-26
This bug affects 42 people. Does this bug affect you?
212
Affects
Status
Importance
Assigned to
Milestone
net-snmp (Ubuntu)
Invalid
Undecided
Unassigned
Target to milestone
Bionic
Invalid
Undecided
Unassigned
Target to milestone
Cosmic
Invalid
Undecided
Unassigned
nodejs (Ubuntu)
Invalid
Undecided
Unassigned
Target to milestone
Bionic
Invalid
Undecided
Unassigned
Target to milestone
Cosmic
Invalid
Undecided
Unassigned
openssl1.0 (Ubuntu)
Won't Fix
Medium
Unassigned
Target to milestone
Bionic
Won't Fix
Medium
Unassigned
Target to milestone
Cosmic
Invalid
Medium
Unassigned
Report a bug
This report contains Public information
Everyone can see this information.
Mark as duplicate
Convert to a question
Link a related branch
Link to CVE
Change lock status
Duplicates of this bug
Bug #1873608
You have subscriptions that may cause you to receive notifications, but you are not directly subscribed to this bug's notifications.
Mute bug mail
Edit bug mail

ABI changes are hard

- LTS distros set ABI
- 3rd party ecosystems target those ABIs
- Breaking ABI not acceptable
- Adding ABI often is not OK either
- Deprecating ABI is often impossible
- Runtime behaviour changes often the easiest to land

OpenSSL ABI is unstable

- Config options change public ABI
- Config options change runtime behaviour
- Test suite expects deprecated features to work
- Test suite expects museum cryptography to work
- Bind-now / Apps expect Engine API to be present
- Nodejs expects and often loads legacy provider
- Webpack tries to use MD4
- Config options often do not apply to libcrypto
- Minimum / floor settings not enforced

Shipping latest OpenSSL

- Just ship latest OpenSSL?
- Rolling distros / Intel Clear Linux / Chainguard
- Requires extensive testing
- Chainguard spins up 10,000+ kubernetes clusters
- Compatibility with OpenSSL FIPS provider sometimes breaks
- Compatibility with Symcrypt / Wolfcrypt / etc sometimes breaks
- Performance behind forks of OpenSSL (boringcrypto, aws-lc, cloudflare)
- Behind in features for Hybrid-PQC, PQC, QUIC
- Easier to accumulate ABI, very hard to drop ABI

History for os / **openssl.yaml** on `main`

All users | All time

Commits on Oct 7, 2025

openssl/3.6.0 package update (#67840)
octo-sts[bot] authored 5 hours ago · ✓ 6 / 6
Verified a087551

Commits on Oct 2, 2025

openssl/3.5.4 package update (#67728)
octo-sts[bot] and wolfi-bot authored 5 days ago · ✗ 6 / 9
Verified 335661f

Commits on Sep 30, 2025

openssl: restore 3.5.3 once again (#67715)
sil2100 authored last week · ✗ 6 / 9
Verified 92beffe

Temprorary downgrade openssl
xnox committed last week · ✗ 4 / 12
Verified 6f9e1c8

openssl: bump 3.5.3 due to withdrawal
sil2100 committed last week · ✓ 11 / 13
Unverified a4197d4

openssl/3.5.3 package update (#66266)
3 people authored last week · ✗ 6 / 9
Verified 68eec63

Fun shipping latest OpenSSL

- Land 3.5.3
- Broke OpenSSH version check
- Withdraw 3.5.3
- Remove bogus OpenSSH version
- Reland 3.5.3, land 3.5.4, land 3.6.0

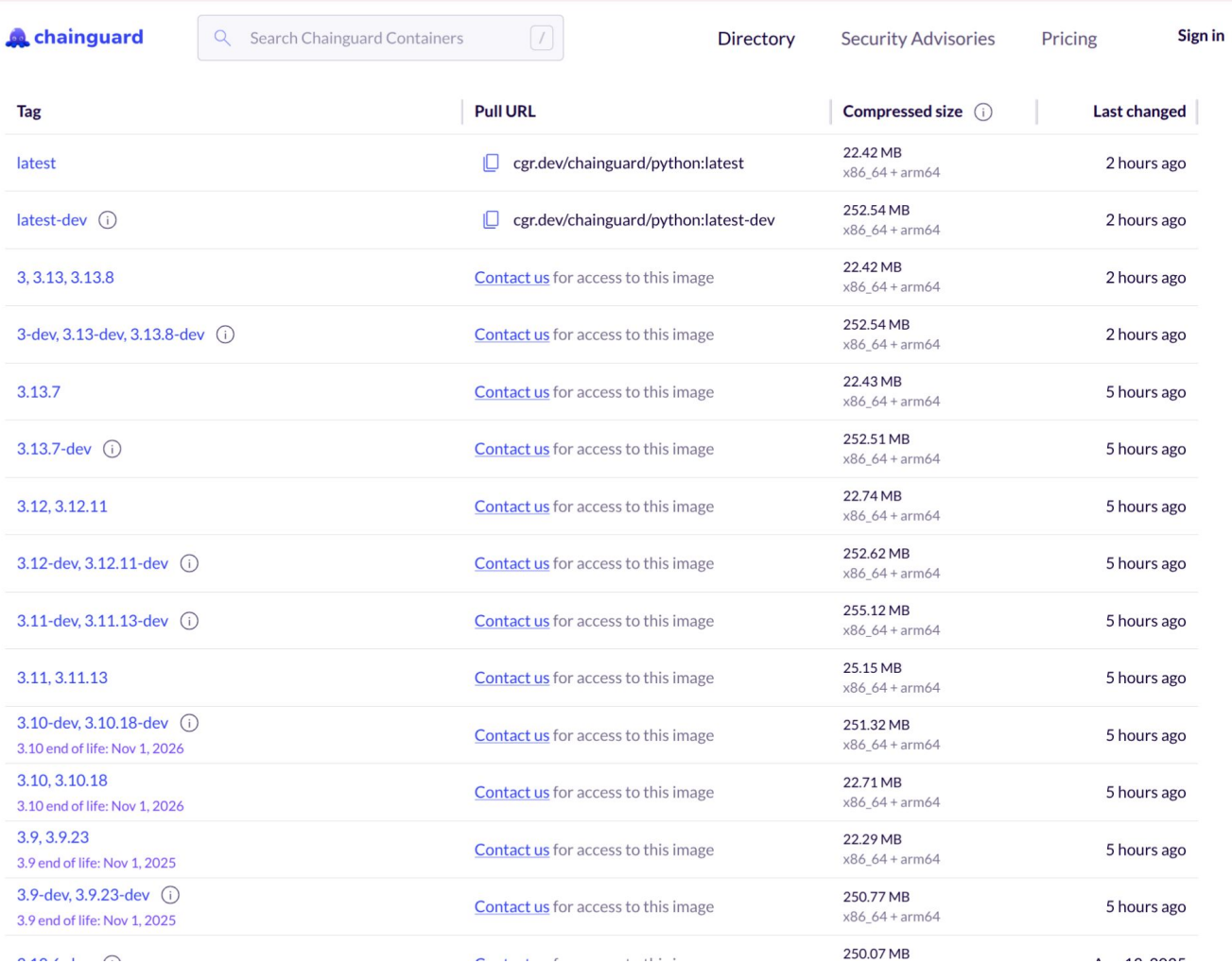
- Rebuild ~1,700+ project containers, two arches, all version streams
- Deploy 10,000+ kubernetes clusters to test all combinations everything
- FIPS providers: 3.1.2; 3.4.0; 3.6.0

Eliminate your CVEs

Build, ship, and run secure software with minimal, hardened container images — rebuilt from source daily and guarded under our industry-leading remediation SLA.

Projects	Versions	Images	Builds
1,755	104,547	207,246	304,702,747

Search Chainguard Containers /



Tag	Pull URL	Compressed size	Last changed
latest	cgr.dev/chainguard/python:latest	22.42 MB x86_64 + arm64	2 hours ago
latest-dev	cgr.dev/chainguard/python:latest-dev	252.54 MB x86_64 + arm64	2 hours ago
3, 3.13, 3.13.8	Contact us for access to this image	22.42 MB x86_64 + arm64	2 hours ago
3-dev, 3.13-dev, 3.13.8-dev	Contact us for access to this image	252.54 MB x86_64 + arm64	2 hours ago
3.13.7	Contact us for access to this image	22.43 MB x86_64 + arm64	5 hours ago
3.13.7-dev	Contact us for access to this image	252.51 MB x86_64 + arm64	5 hours ago
3.12, 3.12.11	Contact us for access to this image	22.74 MB x86_64 + arm64	5 hours ago
3.12-dev, 3.12.11-dev	Contact us for access to this image	252.62 MB x86_64 + arm64	5 hours ago
3.11-dev, 3.11.13-dev	Contact us for access to this image	255.12 MB x86_64 + arm64	5 hours ago
3.11, 3.11.13	Contact us for access to this image	25.15 MB x86_64 + arm64	5 hours ago
3.10-dev, 3.10.18-dev 3.10 end of life: Nov 1, 2026	Contact us for access to this image	251.32 MB x86_64 + arm64	5 hours ago
3.10, 3.10.18 3.10 end of life: Nov 1, 2026	Contact us for access to this image	22.71 MB x86_64 + arm64	5 hours ago
3.9, 3.9.23 3.9 end of life: Nov 1, 2025	Contact us for access to this image	22.29 MB x86_64 + arm64	5 hours ago
3.9-dev, 3.9.23-dev 3.9 end of life: Nov 1, 2025	Contact us for access to this image	250.77 MB x86_64 + arm64	5 hours ago
		250.07 MB	

What can be done better?

- Port upstream projects away from deprecated API / ABI
- Ensure stable public ABI irrespective of no-* options
  - Enable builds with deprecated-stubs (glibc style)
  - E.g. keep ENGINE symbols, hide them for new linking
  - E.g. keep ENGINE symbols, but do nothing / return success
- Status quo, turning off TLSv1.1, deprecated API will break
  - Python
  - Nodejs
  - .NET

Ensure conflict-free patches

- Keep NEWS / CHANGES / doc changes separate
- Often conflict on cherry-pick / backport
- Automatic cherry-pick fails, requiring human intervention
- Downstream has own changelogs / git / %changes / etc
- Consider using changelog snippet files (see cpython)
- Consider to generate News/Changes from git log
- Consider enforcing News/Changes in stand-alone commits

Help security scanners

- Security scanners expect release versions
- Building from tag/tarball helps with automation
- Consider fully automatic stable releases every week
- Consider to always tag security fixes
- Such that security patches can always be referred by a tagged version
- For all supported branches, and merge to stable branch

Questions?

How to enable TLSv1.1 TLSv1.0 on 20.04 LTS?
How to disable TLSv1.1 TLSv1.0 on 18.04 LTS?

Keeps going up and down in popularity