BSD News
August 2019
REPORTS & UPDATES
LibreSSL 3.0.0 Released in OpenBSD

List: openbsd-announce
Subject: LibreSSL 3.0.0 Released
From: Brent Cook <busterb () gmail ! com>
Date: 2019-08-05 12:43:56
Message-ID: 20190805124356.GA38208 () santodn1an

We have released LibreSSL 3.0.0, which will be arriving in the
LibreSSL directory of your local OpenBSD mirror soon.

This is the first development release from the 3.0.x series, which will
eventually be part of OpenBSD 6.6. It includes the following changes:

- Completed the port of RSA_METHOD accessors from the OpenSSL 1.1 API.
- Documented undescribed options and removed unfunctional options
description in openssl(1) manual.
- A plethora of small fixes due to regular oss-fuzz testing.
- Various side channels in DSA and ECDSA were addressed. These are some of
  the many issues found in an extensive systematic analysis of bignum usage
  by Samuel Weiser, David Schrammel et al.
- Enabled openssl(1) speed subcommand on Windows platform.
- Enabled performance optimizations when building with Visual Studio on Windows.
- Fixed incorrect carry operation in 512 addition for Streebog.
- Fixed -modulus option with openssl(1) dsa subcommand.
- Fixed PVK format output issue with openssl(1) dsa and rsa subcommand.

The LibreSSL project continues improvement of the codebase to reflect modern,
safe programming practices. We welcome feedback and improvements from the
broader community. Thanks to all of the contributors who helped make this
release possible.

Source: https://marc.info/?l=openbsd-announce&m=156500965928485&w=2
OpenZFS on OS X 1.9.2 released

- Fixed some core dumps & aborts after `zfs rename`
- Fixes in:
  - `zfs raw recv`
  - `zfs spill block recv`
  - `zfs send deadlock in bqueue`

Source: https://openzfsonosx.org/forum/viewtopic.php?f=20&t=3296
OpenBSD binary updates for security and other problems in Base OS

- **release**: fixed point in time, no update (6.3, 6.4, 6.5, ...).
- **stable**: conservative updates only. For ports, only the most recent release is updated (currently 6.5).
- **current**: main development branch, receives bigger changes.

---

**List:** openbsd-announce

**Subject:** OpenBSD-stable binary packages

**From:** Release Manager <release@openbsd.org>

**Date:** 2019-08-14 10:29:24

**Message-ID:** 926b5261e19b8c157f1 @ solene / perso / local

The OpenBSD base system has received binary updates for security and other important problems in the base OS through syspatch16 for the last few releases.

We are pleased to announce that we now also provide selected binary packages for the most recent release. These are built from the -stable ports tree which receives security and a few other important fixes:

- **release**: fixed point in time, no update (6.3, 6.4, 6.5, ...).
- **stable**: conservative updates only. For ports, only the most recent release is updated (currently 6.5).
- **current**: main development branch, receives bigger changes.

Initial updates for 6.3-6.5 are already available at most mirrors (check for the /OpenBSD-6.5/packages-stable directory). 6.6 is currently in testing, and 6.7 is planned to be released in 2020. If you are using is not synced yet, you will need to wait or use a different one.

**pkg_add()** already has the required heuristic to manage -stable packages. It will be able to use /OpenBSD-6.5/packages-stable directory in the following two ways:

1. You can just `install()` and the `PKG_PATH` environment variable is not set (default installation case).
2. You use the `PKG_PATH` environment variable and it uses `6.5` or `6.6`.

The two directories are separate because the `packages` directory holds the packages built at the release time. They will not be updated.

The packages-stable directory will be early update at the time of a new release. Its contents will grow during the release life cycle as security fixes and other fixes are committed to the -stable ports tree.

If `pkg_add()` installs a new package and you meet the conditions for using the packages-stable directory, detailed above, the version in packages-stable will be chosen instead of the original supplied at release time. This also applies when using `pkg_add -u` to upgrade packages.

This means that, in a default installation, `pkg_add` will automatically pick the latest version available to you.

In the case of updating an installed package, this may require restarting the running binaries to use the new code.

More info on the package system can be found at the following link:
https://www.openbsd.org/faq/faq15.html

Surprisingly, nobody saw the new directory show up on our mirrors, and then report it on our mailing lists.

**Source:** https://marc.info/?l=openbsd-announce&m=156577865917831&w=2
OpenBSD Ada bindings for pledge & unveil

This library was written to help my easing into Ada programming, as I struggle with this language so different from all others I’ve known. This is a package I can be proud of, however. This defines a simple package for OpenBSD’s extra facilities, namely pledge and unveil. There is an enumeration type common to both, two more enumeration types, two array types thereof, two exceptions, and then two procedures Pledge and Unveil. This is a simple and high-level interface to OpenBSD’s pledge and unveil facilities that came to mind in my errant thought. The procedures are expected and designed to be used exclusively with array aggregates and not with the type names. Here is the example that inspired the library:

```ada
with OpenBSD; use OpenBSD;
...
Unveil('/tmp/', (Read => Allowed, others => Disallowed));
...
Pledge(Stdio | Fattr => Allowed, others => Disallowed));
```

These procedures work by fixing Ada’s enumeration types over the strings OpenBSD uses to approximate such a language facility. The pledge accepts a simple string of designated keywords separated by spaces and terminated according to the usual C convention. The unveil accepts a filename and string of designated characters terminated according to the usual C convention, as well. Failure cases are invalid pointers, malformed strings, invalid requests, attempts to increase permissions, and so on. Several of these failure cases simply won’t occur in Ada; the permission errors are those that are particularly relevant and correspond to the exceptions, with unveil confining some of the failure cases for simplicity, and this is a reasonable decision given that the precise error can be learned.

I’m, of course, still rather green to Ada and so it can be expected the body of this package will be improved over time. I likely won’t change any of the names used in the specification, but this is a reason you should only use array aggregates with it. This library is not currently robust to change as I believe it should be, but I intend to correct this. It has been a valuable learning experience and I expect to update this library as OpenBSD changes the semantics of pledge and unveil or adds new facilities that would be worthwhile to expose to Ada.

Here is the package specification, the package body, and the documentation.

Written in 2019 by Prince Trippy.

This page is available under the CC0 Public Domain Dedication.

Source: http://verisimilitudes.net/2019-07-27
New firewall test suite on FreeBSD

Revision 350586

Jump to revision: 350586 Go

Author: thj
Date: Mon Aug 5 11:47:34 2019 UTC (2 weeks, 2 days ago)
Changed paths: 7

Log Message:
Add common firewall test suite

Add a common test suite for the firewalls included in the base system. The test suite allows common test infrastructure to test pf, ipfw and ipf firewalls from test files containing the setup for all three firewalls.

Add the pass block test for pf, ipfw and ipf. The pass block test checks the allow/deny functionality of the firewalls tested.

Submitted by: Ahsan Barkati
Sponsored by: Google, Inc. (GSoC 2019)
Reviewed by: kp
Approved by: bz (co-mentor)
MFC after: 2 weeks
Differential Revision: https://reviews.freebsd.org/D21065

Source: https://svnweb.freebsd.org/base?view=revision&revision=350586

Test suite for pf, ipfw and ipf;
OpenBSD ported Electron

Bryan Steele 🦋
@canadianbryan

robert@ has ported Electron to OpenBSD by integrating it into our chromium port, it also uses the current stable version and not some older copy, avoiding duplicating some 600+ local patches.

Henry, shield your eyes! @qb1t

Sadly no pledge/unveil.. yet.

Source: https://twitter.com/canadianbryan/status/1164632273519611904?s=19
More updates for using OpenBSD on Lenovo X1

OpenBSD Support Log

2019-07-26: First boot of the OpenBSD installer panicked fairly early with an AML error "Not Integer". Booting a non-ramdisk kernel with ACPI_DEBUG enabled showed this was due to a problem with the touchpad's _INT method. I eventually tracked this down to a problem with OpenBSD's implementation of ToHexString, a fix for which has been been committed.

2019-07-29: Now that the system boots, I noticed that key repeating on the console was broken, and that date; sleep 1; date showed it taking 3 or 4 seconds. In the past this has been due to an unsynchronized TSC, but even with acpi@pm@ being the new default kern.timecounter.hardware, it still showed this problem. Some further debugging pointed to cpu0: apic clock running at 100MHz when it should be 24MHz. By default, the X1 Carbon ships with its BIOS option "8254 Timer Clock Gating" enabled, and OpenBSD uses the 8254 for APIC clock calibration. This was fixed by fetching the CPU frequency directly from the CPU instead of timing it, in order to avoid relying on the 8254.

Despite fixing the jhidov polling issue, the X1C7's touchpad uses GPIO interrupts and requires a new Cannon Lake GPIO driver. I'll need to work on this.

2019-08-07: I realized that the sound from the speakers was lacking bass on OpenBSD but sounded fine on Linux. A tweak with mixerctl will properly hook up the speaker2 outputs to the proper DAC, enabling proper sound on OpenBSD.

    echo outputs.spkr2_source-dac-8:1 >> /etc/mixerctl.conf

2019-08-13: I committed a quirk to the azalia driver to do the speaker routing by default without having to use mixerctl.

- lacking bass on OpenBSD;
- fix for msrs & pat on main CPU -- slow console on x1r7.

Source: https://jcs.org/2019/08/14/x1c7
Example reports for anyone:

- **not a programmers:**
  - link to a presentation of the 2019 FreeBSD survey results at BSDCan 2019

- **more technical:**
  - news about git in FreeBSD;
  - status of some error detection on security tools,
  - announce the sysctl clone

- **experienced:**
  - updates to the linux compatibility layer;
  - much low level work on graphics;
  - many new bhyve features;
  - more user-friendly experience with trackpoints and touchpads enabled by default

BUGS
Reported CVE in BSD

- Reference count overflow in mqueue (FreeBSD 11.2 - 12.0) [CVE-2019-5603]
- Kernel memory disclosure from /dev/midistat (FreeBSD 11.2 - 12.0) [CVE-2019-5612]
- IPv6 remote Denial-of-Service (FreeBSD 11.2 - 12.0) [CVE-2019-5611]
- Insufficient validation of guest-supplied data (e1000 device) (FreeBSD 11.2 - 12.0) [CVE-2019-5609]
- Insufficient message length validation in bsnmp library (FreeBSD 11.2 - 12.0) [CVE-2019-5610]
- ICMPv6 / MLDv2 out-of-bounds memory access (FreeBSD 11-2 - 12.0) [CVE-2019-5608]
- Multiple vulnerabilities in bzip2 (FreeBSD 11.2 - 12.0) [CVE-2016-3189, CVE-2019-12900]
Reported errata

- ipfw(8) jail keyword broken prior to jail startup

- Bhyve instruction emulation improvements (opcode 03H and F7H)

- Incorrect exception handling in libunwind (FreeBSD 11.2, 12.0)

- Incorrect locking in epoch(9)

- IPv6 neighbor cache leak on expiration (NetBSD 8.1 - current)
CURIOSITIES
New GSoC update for incorporating the memory-hard Argon2 hashing scheme into NetBSD

Report contains some recommendations and descriptions for:

- Argon2 variants;
- appropriate salt length;
- appropriate tag length;
- appropriate degree of parallelism;
- maximum amount of memory to utilize;
- acceptable time cost;

Source: https://blog.netbsd.org/tnf/entry/gsoc_2019_report_update_incorporating
Fuzzing NetBSD filesystems via AFL [Part 2]

Report contains information about:

- AFL port for NetBSD;
- plans to write a kernel fuzzing benchmark;
- step by step examples how to fuzzing particular filesystem

Source: http://blog.netbsd.org/tnf/entry/fuzzing_netbsd_filesystems_via_afl
Half-Life 1 on OpenBSD -- confirmed

Looks like @thfrw played some Half-Life 1 (xash3d) on #OpenBSD but neglected to tweet about it.

#PlayOnBSD

Source: https://twitter.com/canadianbryan/status/1158512880217731079
OpenBSD Olive: Adobe Premiere-like clone

(((Dr. Brian Robert Callahan)))
@__briancallahan

Must be a video editing weekend. Got Olive, an Adobe Premier-like clone, working on #OpenBSD too!

Source: https://twitter.com/__briancallahan/status/11577847381299752067
OpenBSD 6.5 booted from floppy disk on machine from 1996

- Successful network installation of OpenBSD 6.5 + LibreSSL + Perl.
- Machine specification:
  - Pentium 200 (Socket 7, no MMX),
  - 128 MB RAM, 4x SIMM,
  - 1 MB DRAM for integrated graphic S3 Trio64+.
- Installer size: ~ 1.44 MB.

Source:
New VCS on OpenBSD: Game of Trees

Game of Trees

Contributed by cuider on 2019-08-10 from the got-to-do-things-property dept.

Stefan Sperling (stsp) is developing a version control system, "Game of Trees". From <https://gameoftrees.org/>

Game of Trees (Got) is a version control system which prioritizes ease of use and simplicity over flexibility.
Got is still under development; it is being developed exclusively on OpenBSD and its target audience are OpenBSD developers.
Got uses Git repositories to store versioned data. At present, Got supports local version control operations only. Git can be used for any functionality which has not yet been implemented in Got. It will always remain possible to work with both Got and Git on the same repository.

GoT has been added to the ports tree as dev/ree. 
It is the subject of a talk at EUROBSDCON 2019.
Stefan has been involved in the discussion on Lobster.

Source: https://unde考验.org/cgi?action=article;sid=20190810123007
EVENTS
BSD Events in August

August 2019

- **COSCUP 2019**, Taipei, Taiwan
  17 - 18 August, 2019

- **Open Source Summit North America**, San Diego, United States
  21 - 23 August, 2019
BSD Events in September

September 2019

- vBSDcon 2019
  September 5-7, 2019, Reston, VA, USA.

- EuroBSDCon 2019