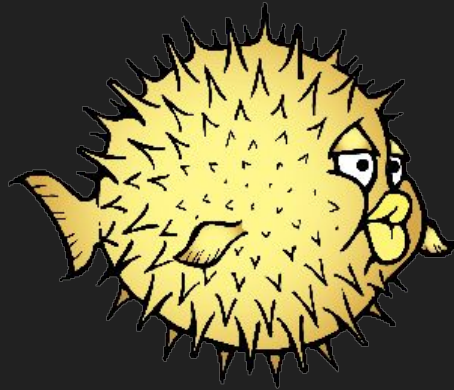


# BSD News

December\* 2019

Michał Borysiak





OpenBSD

# OpenSSH U2F/FIDO support in base

- U2F support in base
- Hardware backed keys can be generated using `ssh-keygen -t [ecdsa-sk|ed25519-sk]`
- Private key contain a key handle used by security key to deliver the real private key
- Can be added to agent or authorized keys



<https://undeadly.org/cgi?action=article;sid=20191115064850>

# System call origin verification

- Hardens against attacks basing on W^X failures and JIT bugs
- System call must be done from a registered memory location (libc)
- Process is killed
- New system call: mysyscall(2)
- Eventually it will block any system call attempt made outside libc and ld.so
- Allowed regions: code segment, libc\*, ld.so\*
- Go calls system directly
- Breaks ABI compatibility

# Authentication vulnerabilities

- CVE-2019-19521: Authentication bypass: smtpd, ldapd, radiusd, sshd\*, su\*
- CVE-2019-19520: Local privilege escalation via xlock
- CVE-2019-19522: Local privilege escalation via S/Key and YubiKey
- CVE-2019-19519: Local privilege escalation via su
- Patches were available after 40 hours after initial contact

# Local Privilege Escalation in dynamic loader

- CVE-2019-19726
- Local Privilege Escalation in OpenBSD's dynamic loader (ld.so)
- Can be exploited via set-user-ID binaries (like passwd)
- “Overloaded” LD\_LIBRARY\_PATH variable is ignored but not deleted from the environment
- Patches were available after 3 hours

# Firefox for 6.6-stable won't receive updates

- Too complex to package on the stable branch: rust dependencies
- It would require testing many rust dependencies
- It will remain vulnerable for CVE-2019-17026
- Switch to firefox-esr or upgrade system to current

## Mozilla Foundation Security Advisory 2020-03

### Security Vulnerabilities fixed in Firefox 72.0.1 and Firefox ESR 68.4.1

**Announced** January 8, 2020

**Impact** critical

**Products** Firefox, Firefox ESR

**Fixed in** Firefox 72.0.1  
Firefox ESR 68.4.1

#### # CVE-2019-17026: IonMonkey type confusion with StoreElementHole and FallibleStoreElement

**Reporter** Qihoo 360 ATA

**Impact** critical  
**Description**

Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild abusing this flaw.

#### References

[Bug 1607443](#)

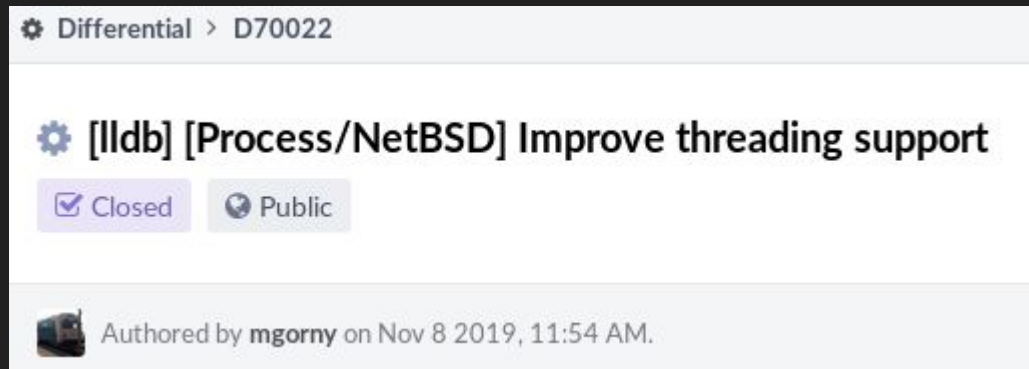
<https://undeadly.org/cgi?action=article;sid=20200109141600>





# NetBSD LLVM changes

- LLDB threading support
- Clang built bot 2-stage builds
- NetBSD supports LLVM development




The screenshot shows a patch titled "[lldb] [Process/NetBSD] Improve threading support" with a status of "Closed" and "Public". It was authored by mgorny on Nov 8 2019, 11:54 AM.

Differential > D70022

**[lldb] [Process/NetBSD] Improve threading support**

Closed  Public

 Authored by mgorny on Nov 8 2019, 11:54 AM.

[https://blog.netbsd.org/tnf/entry/clang\\_build\\_bot\\_now\\_usage](https://blog.netbsd.org/tnf/entry/clang_build_bot_now_usage)

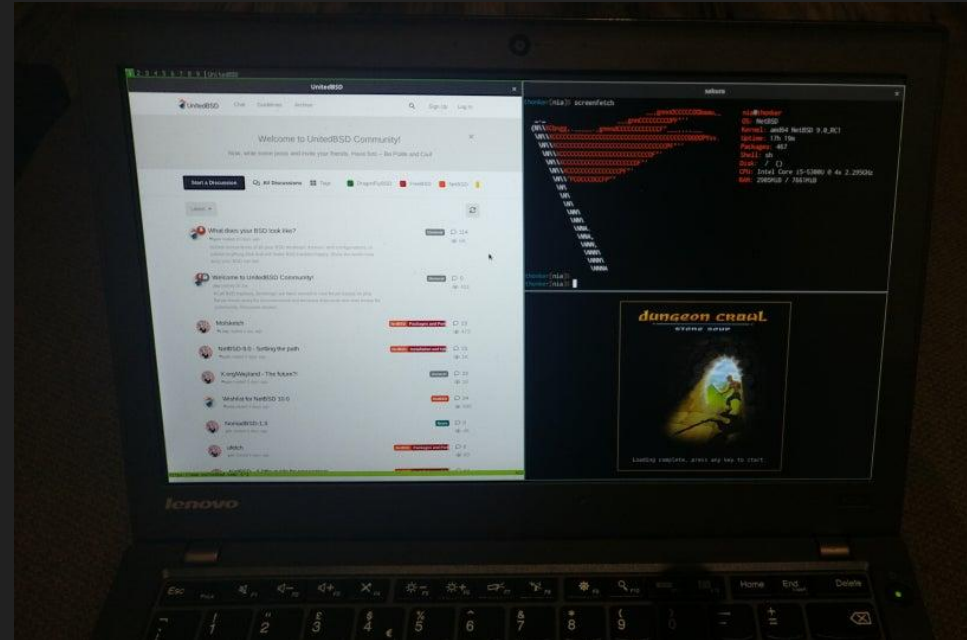
# NetBSD 9.0 RC-1 available

- Kernel ASLR
- Kernel leak detector
- Kernel Address Space Sanitizer
- Kernel Undefined Behavior Sanitizer
- User space sanitizers
- ZFS update

[https://blog.netbsd.org/tnf/entry/first\\_release\\_candidate\\_for\\_netbsd](https://blog.netbsd.org/tnf/entry/first_release_candidate_for_netbsd)

# Wayland/WebRTC support in NetBSD 9/Linux

- WebRTC enabled by default for some firefox packages
- Wayland enabled by default for a few packages required to install a Wayland compositor
- Try Wayland using wm/velox compositor
- NetBSD 9.0 RC-1 + velox on Thinkpad X250



<https://mail-index.netbsd.org/pkgsrc-users/2020/01/05/msg030124.html>

[https://www.reddit.com/r/BSD/comments/eb1eoq/new\\_laptop\\_thinkpad\\_x250\\_netbsd\\_90\\_rc1\\_velox/](https://www.reddit.com/r/BSD/comments/eb1eoq/new_laptop_thinkpad_x250_netbsd_90_rc1_velox/)

# How to use pkgsrc on Linux

- NetBSD is famous for running on basically anything
- Over 20 operating systems are supported: BSD, Illumos, Solaris, Mac ... and also Linux



<https://opensource.com/article/19/11/pkgsrc-netbsd-linux>



freeBSD®

# GEOM NOP

- Test other GEOM classes
- GEOM NOP can simulate I/O errors with a given probability
- Incoming changes

**oshogbo//vx**  
*My place in space*

## GEOM NOP

Nov. 18, 2019, 3:41 p.m.



FreeBSD

Differential > D22304

gnop: add the option for adding a suffix to the name of the device

Closed

Public

<https://oshogbo.vexillum.org/blog/71/>

# FreeBSD Foundation got \$2,267,306

FreeBSD Foundation 2019 Target Was \$1.25M - they Got \$2.27M instead.



Amount Raised: \$2,267,306

Goal: \$1,250,000

Donors: 757



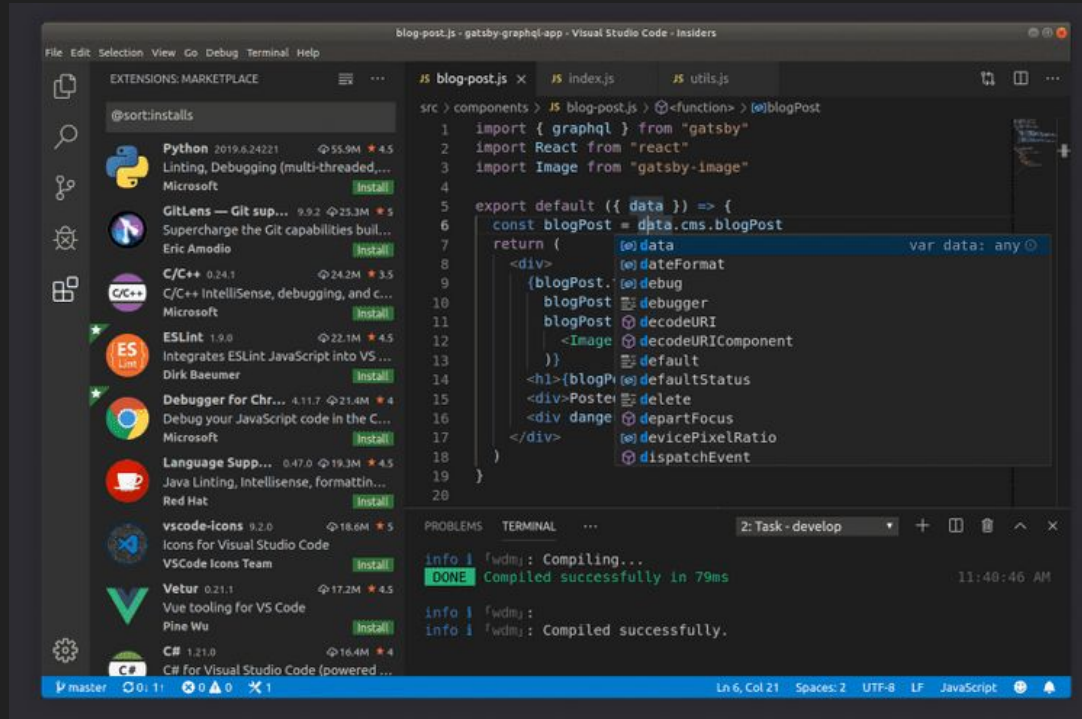
<https://www.freebsdoundation.org/blog/2019-fundraising-update-thank-you/>

# ZFS on Linux renamed to OpenZFS

- It will contain ZFS code for both: Linux and FreeBSD
- OpenZFS 2.0 expected in 2020
- OpenZFS 3.0 expected in 2021 with MacOS support
- Linus Torvalds: Don't use ZFS



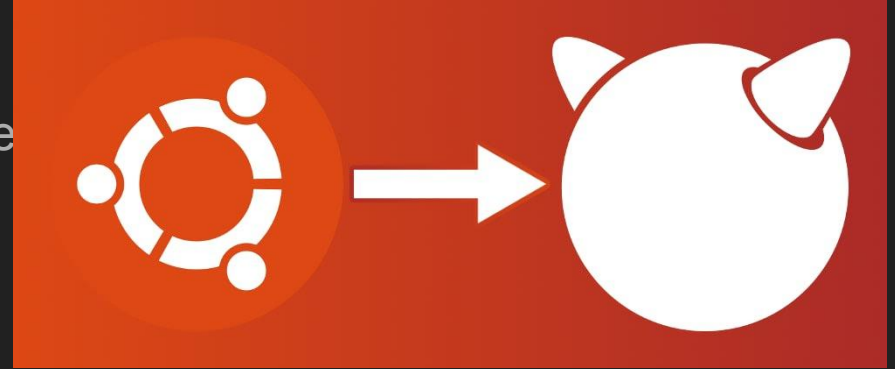
# Visual Studio Code port



<https://www.freshports.org/editors/vscode/>

# Moving away from Ubuntu: peeking at FreeBSD (3 parts)

- Web server with PHP support and MySQL
- FreeBSD as desktop system
- FreeBSD from a beginner perspective
- Good entry point to start with FreeBSD



# NFS 4.2

- Working on NFS over TLS

## Revision 355677

Jump to revision:



**Author:** rmacklem

**Date:** Thu Dec 12 23:22:55 2019 UTC (*4 weeks, 3 days ago*)

**Changed paths:** **18**

**Log Message:**

Add support for NFSv4.2 to the NFS client and server.

This patch adds support for NFSv4.2 (RFC-7862) and Extended Attributes (RFC-8276) to the NFS client and server.

NFSv4.2 is comprised of several optional features that can be supported in addition to NFSv4.1. This patch adds the following optional features:

- posix\_fadvise(POSIX\_FADV\_WILLNEED/POSIX\_FADV\_DONTNEED)
- posix\_fallocate()
- intra server file range copying via the copy\_file\_range(2) syscall  
--> Avoiding data transfer over the wire to/from the NFS client.
- lseek(SEEK\_DATA/SEEK\_HOLE)
- Extended attribute syscalls for "user" namespace attributes as defined by RFC-8276.

<https://svnweb.freebsd.org/base?view=revision&revision=355677>

# KTLS example usage

- KTLS added to FreeBSD a few months ago
- Sendfile(2) over TLS
- Interesting question about using KTLS to transfer NFS over TLS

## how to use the ktls

**John Baldwin** [jhb at FreeBSD.org](mailto:jhb@FreeBSD.org)

*Wed Jan 8 18:08:38 UTC 2020*

- Previous message (by thread): [how to use the ktls](#)
  - Next message (by thread): [how to use the ktls](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)
- 

<https://lists.freebsd.org/pipermail/freebsd-current/2020-January/075064.html>

# 11 years without an upgrade



**Edwin Kremer**  
@EdwinKremer

Follow

Colleague of mine asked the other day if I could possibly remember how I set up a #FreeBSD server back in 2008. So I took a look at the box and found this! That's just over 11 years (!), shoveling IP packets left, right and center.

#RockStable

#WhatIsAMemoryLeakAnyway

#LoveBSD

```
copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
  The Regents of the University of California. All rights reserved.

FreeBSD 7.0-RELEASE (NOVA_R200) #0: Tue Apr  8 09:56:02 UTC 2008

sh (the default Bourne shell in FreeBSD) supports command-line editing.  Just
''set -o emacs'' or ''set -o vi'' to enable it.
novazembla:/etc-:
novazembla:/etc-:
novazembla:/etc-: uptime
12:08PM up 4017 days, 1:04, 1 user, load averages: 0.00, 0.00, 0.00
novazembla:/etc-: █
```

2:00 PM - 6 Dec 2019

<https://twitter.com/EdwinKremer/status/1203071684535889921>

Thank you for your attention!

