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

https://undeadly.org/cgi?action=article;sid=20191202105849
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

- To 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

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
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/eb1eog/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
GEOM NOP

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

https://oshogbo.vexillium.org/blog/71/
FreeBSD Foundation got $2,267,306

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

https://www.freebsdfoundation.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

https://zfsonlinux.topicbox.com/groups/zfs-discuss/T13eecd32607dab41
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

https://dev.to/jmmedina00/moving-away-from-ubuntu-peeking-at-freebsd-part-1-2jne
NFS 4.2

- Working on NFS over TLS

Revision 355677

Jump to revision: 355677

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 syscall 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

11 years without an upgrade

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

https://twitter.com/EdwinKremer/status/1203071684535889921
Thank you for your attention!