OpenBSD 6.3 mit Schutz vor Meltdown & Co.

Schmelzfrei

Michael Plura

Mit Version 6.3 entschärfen die OpenBSD-Entwickler die Bedrohung durch Meltdown/Spectre, erweitern den systemeigenen Hypervisor *vmm* und machen ARM64 zur offiziell unterstützten Plattform.

Zwei Wochen früher als geplant veröffentlichte das Team seine inzwischen 44. Release: OpenBSD 6.3. Im Zentrum stehen Maßnahmen zum Entschärfen der Meltdown/Spectre-Sicherheitslücken in Intel-CPUs ab Baujahr 1995 und Cortex-A75-Prozessoren. Für OpenBSD 6.2 gibt es einen über *syspatch* installierbaren Fix (siehe ix.de/ix1805068).

Wie bei Linux erreicht OpenBSD dies unter anderem durch Kernel Page Table Isolation (KPTI) und spezielle Behandlung des Branch Target Buffer (BTB). Um nachträgliche Fehlerbehebungen für Intel-CPUs zu ermöglichen, lassen sich die beim Systemstart via *fw_update* mit aktuellem Microcode versehen.

Dazu erweiterten die Entwickler das mit OpenBSD 6.2 eingeführte „Trapsled“, das die von Angreifern gerne ausgenutzten „NOP-Rutschen“ durch INT13-Befehle und einen Sprung über diese ersetzt, auf weitere Architekturen. Weiter schränken sie mit *pledge* Zugriffe eines Programms auf nicht benötigte Systemaufrufe ein. Ein zweiter Parameter *execpromises* kann dies nun auch für Kindprozesse definieren. Einen via *crontab –e* verwendeten Emacs kann man so aus dem *crontab*-Sourcecode heraus daran hindern, eine Shell aufzurufen – was ihm sonst durchaus erlaubt wäre (siehe ix.de/ix1805068).

Bereits seit einiger Zeit arbeitet das OpenBSD-Team daran, *KERNEL_LOCK()* aus dem Netzwerk-Stack zu entfernen, um diesen weiter zu parallelisieren. OpenBSD 6.3 verarbeitet eingehende TCP/UDP-Pakete und IPsec nun ohne diese Bremse, was bei einem ersten Test spürbar mehr Durchsatz und geringere Latenzzeiten etwa auf einer OpenBSD-Firewall bringt. GRE (Generic Routing Encapsulation) ist nun über IPv6 möglich, mit *egre* gibt es einen Treiber für Ethernet-over-GRE-Tunnel und mit *nvgre* einen Treiber für Netzwerkvirtualisierung.

Verbesserungen der Intel-WiFi-Treiber *iwm* und *iwn* beheben diverse Probleme aktueller Intel-Chipsätze für Notebooks. OpenBSD 6.3 unterstützt auch die GBit-Schnittstellen (Intel PRO/1000) von Intels Cannonlake und Icelake.

IPv6-Clients erhalten via *slaacd* (Stateless Address Autoconfiguration Daemon) automatisch konfigurierte Adressen gemäß RFC 7217, wobei alle durch RFC 4862 vorgegebenen Präfixlängen berücksichtigt werden.

Hypervisor aufgebohrt

Auch der Hypervisor *vmm* erfuhr eine deutliche Erweiterung und besitzt nun eine ordentliche Fehlerbehandlung. Optische Medien des Hosts oder ISO-Images lassen sich via *vioscsi* einbinden, und eine VM kann bis zu vier virtuelle Netzwerkkarten ansprechen. Einige bestehende VMs müssen Nutzer beim Upgrade von OpenBSD 6.2 auf 6.3 umkonfigurieren. Der Hypervisor erzeugt die in der Konfiguration *(vm.conf)* definierten Netzwerkbrücken nicht mehr selbstständig. Stattdessen sind diese vorab durch Anlegen einer Datei wie */etc/hostname.bridge0* einzurichten.

Mit *vmt* lassen sich auf AMD-SVM/RVI-Hosts Clones und Snapshots laufender VMs anlegen. 32-Bit-Linux-Gäste finden ein besseres PAE vor, außerdem unterstützt OpenBSD 6.3 ukvm/Solo5 Unikernel (MirageOS) – eine Art Minimalisierung für Cloud-Instanzen (siehe ix.de/ix1805068).

ARM64 ist offizielle Plattform

Auf der ARM64-Plattform (beispielsweise PINE64, Orange Pi PC2, Firefly RK3399 und Raspberry Pi 3) nutzt OpenBSD dank stabilem SMP-Support nun alle Kerne. Bei ARMv7 (32-Bit, unter anderem Cubieboard, Banana Pi, BeagleBone) kann das System nun die FPU (VFP, Vector Floating Point) und die SIMD-Erweiterung (NEON, Media Processing Engine) nutzen, was vor allem mathematische Berechnungen und das De- und Encoding von Multimediainhalten beschleunigt. Es gibt viele neue Treiber für ARM-Chips, etwa für den Zufallszahlengenerator und die Temperatursensoren der Broadcom BCM2835/6/7 oder die Host/PCIe-Bridge des Rockchip RK3399. Bereits Anfang Dezember erhielt ARM64 den Status einer offiziell unterstützten Plattform. Auch die Umstellung vom angestaubten *gcc* auf LLVM/Clang 5.0.1 ist bei ARM64 nahezu abgeschlossen.

Unmengen von Verbesserungen sind naturgemäß in die OpenBSD-Projekte OpenSMTP 6.0.4, OpenSSH 7.7 und LibreSSL 2.7.2 eingeflossen. Sämtliche Änderungen sind in den Release Notes aufgeführt, Tipps zum Wechsel von OpenBSD 6.2 auf 6.3 im Upgrade Guide (siehe ix.de/ix1805068). (avr@ix.de)

Michael Plura

arbeitet in Schweden als freier Autor mit den Schwerpunkten IT-Sicherheit, Virtualisierung und freie Betriebssysteme.

Alle Links: ix.de/ix1805068