Release Notes

TNOS® 3.2.04

TNOS® 3.2.04
Release Notes

September 2017

doc bd2c8e28b022c0322b1fcb03d761aa2c426bcaf7

Contents

3.2.04 Release Notes

Release History

Version	Release Date
3.2.04	2017-09-29
3.2.03	2017-08-29
3.2.02	2017-08-07
3.2.01	2017-08-04
3.2.00	2017-07-27

Enhancements

3.2.04

- *No enhancements in this release.*

3.2.03

- *No enhancements in this release.*

3.2.02

- *No enhancements in this release.*

  3.2.02 was released for technical reasons only, the version number is the only difference to the previous release. It is safe to skip this update in production deployments.

3.2.01

- Support for the Microsoft Azure Load Balancer has been added (CARP auto-configuration, health, and Azure's SharedConfig property).

3.2.00

- Support for Flow Queue - Controlled Delay (FQ-CoDel) has been integrated into the packet filter. The goal of FQ-CoDel is to provide fair sharing of bandwidth between simultaneous connections and reduce latency differences among them
- Improved existing support for paravirtualised Xen (Amazon EC2), Hyper-V (Microsoft Azure) and virtio (KVM and VMM) interfaces
- Support for paravirtualised Hyper-V (Microsoft Azure) storage has been added
- Initial version of 3.2, based on OpenBSD 6.1

Fixes

3.2.04

- Out of bounds TCB settings may result in a kernel panic. (OpenBSD 6.1 errata 029)
- A buffer over-read and heap overflow in perl's regexp may result in a crash or memory leak. (OpenBSD 6.1 errata 028)
- State transition errors could cause reinstallation of old WPA keys. (OpenBSD 6.1 errata 027)

3.2.03

- SMAP enforcement could be bypassed by userland code. (OpenBSD 6.1 errata 026)
- Avoid the possibility of parent class accumulating stale child classes on it's active list with HFSC.
- Correct a race condition with HFSC scheduling.
- Various changes to improve the robustness of the switch psuedo interface.
- Correct the error handling of short packets on IPsec-enabled bridges.

3.2.02

- *No fixes in this release.*

3.2.01

- An out of bounds read could occur during processing of EAPOL frames in the wireless stack. Information from kernel memory could be leaked to root in userland via an ieee80211(9) ioctl. (OpenBSD 6.1 errata 025)
- A race condition in sosplice() may result in a kernel memory leak. (OpenBSD 6.1 errata 024)

- An integer overflow in wsdisplay_cfg_ioctl() may result in an out-of-bounds read. (OpenBSD 6.1 errata 023)
- An uninitialized variable in fcntl() may result in an info leak. (OpenBSD 6.1 errata 022)
- An uninitialized variable in ptrace() may result in an info leak. (OpenBSD 6.1 errata 021)
- Missing socket address validation from userland may result in an info leak. (OpenBSD 6.1 errata 020)
- With an invalid address family, tcp_usrreq() may take an unintended code path. (OpenBSD 6.1 errata 019)
- An alignment issue in recv() may result in an info leak via ktrace(). (OpenBSD 6.1 errata 018)
- An out-of-bound read in vfs_getcwd_scandir() (mainly used for FUSE) may result in a kernel panic or info leak. (OpenBSD 6.1 errata 017)
- A missing length check in sendsyslog() may result in a kernel panic. (OpenBSD 6.1 errata 016)
- Use-after-free can occur related to SIGIO in two drivers. (OpenBSD 6.1 errata 015)

3.2.00

- Distinguish between self-issued certificates and self-signed certificates, so that self-issued certificates verify correctly in a chain. (OpenBSD 6.1 errata 014)
- When pinging an IPv6 link-local address, the reflected packet had ::1 as source address. The echo reply was ignored as it must be from the link-local address. (OpenBSD 6.1 errata 013)
- An unprivileged console user can cause a kernel crash via a wsmux ioctl (OpenBSD 6.1 errata 012)
- Fix an integer overflow in two range checks of display driver only present in the hppa platform (OpenBSD 6.1 errata 011)
- Use fchmod to avoid a race condition in the File::Path Perl module. Fixes CVE-2017-6512. (OpenBSD 6.1 errata 010)
- The kernel could leak memory when processing ICMP packets with IP options. Note that the packet filter blocks such packets by default. (OpenBSD 6.1 errata 009)
- A gap of 1MB is now added between stack and mmap spaces (OpenBSD 6.1 errata 008)
- Incorrect DTLS cookie handling could result in a NULL pointer dereference (OpenBSD 6.1 errata 006)
- Expired packet filter source tracking entries never got removed, leading to memory exhaustion (OpenBSD 6.1 errata 005)
- Kernel software RAID was unable to create useable concatenated volumes as it always set the size of the volume to zero sectors. (OpenBSD 6.1 errata 004)
- A consistency check that could cause programs to incorrectly verify X.509 certificates when using call-backs that return 1 has been reverted (OpenBSD 6.1 errata 003)
- The kernel virtual machine monitor mismanaged floating point contexts (OpenBSD 6.1 errata 002)

- The DHCP service unconditionally echoed the client identifier, preventing some devices from acquiring a lease. (OpenBSD 6.1 errata 001)