Release Notes

TNOS® 3.1.04

© Copyright 2015, 2016, 2017 Esdenera® Networks GmbH
All rights reserved.

TNOS® 3.1.04
Release Notes

May 2017

Esdenera and TNOS are registered trademarks of Esdenera Networks GmbH.

doc 730875dddb9e9b101aee9f2d4925024efbe20ba5

Contents

3.1.04 Release Notes

Release History

Version	Release Date
3.1.04	2017-05-09
3.1.03	2017-04-12
3.1.02	2017-03-10
3.1.01	2017-02-22
3.1.00	2017-02-14

Enhancements

3.1.04

- Resource/Ephemeral disks on AWS and Azure now used for swap

3.1.03

- Improved Xen device support
- Support for IKEv2 and sasync services added to CLI

3.1.01

- Support Azure base64 encoded CustomData

3.1.00

- Initial version of 3.1, based on OpenBSD 6.0

Fixes

3.1.04

- Incorrect DTLS cookie handling in the TLS library could result in a crash (OpenBSD 6.0 errata 022)
- Correct a problem with the creation of concatenated volumes when using software RAID (OpenBSD 6.0 errata 021)

3.1.03

- ELF auxiliary vector storage leaked piece of kernel stack (OpenBSD 6.0 errata 020)
- Fixed packet filter integer overflow when calculating adaptive timeouts, which would cause spuriously expired states under pressure (OpenBSD 6.0 errata 019)

3.1.02

- Correct a potential problem when interactively adding users
- Prevent a man-in-the-middle attack from rogue 802.11 access points when using WPA1 or WPA2 (OpenBSD 6.0 errata 018)

3.1.01

- Correct handling of `no system user <username> password`

3.1.00

- Rewritten support for byte ranges in the HTTP service compared to OpenBSD 6.0. This solves problems with the initial implementation which led to byte ranges being disabled in OpenBSD 6.0 errata 017
- Avoid possible side-channel leak of ECDSA private keys when signing with the cryptographic library (OpenBSD 6.0 errata 016)
- Avoid continual processing of an unlimited number of TLS records in the TLS library (OpenBSD 6.0 errata 015)
- A logic issue in the SMTP service's header parsing could cause SMTP sessions to hang (OpenBSD 6.0 errata 014)
- A protocol parsing bug in the SSH service could lead to unauthenticated memory and CPU consumption (OpenBSD 6.0 errata 013)
- A particular type of memory allocation could cause an integer overflow leading to an infinit loop (OpenBSD 6.0 errata 012)
- A problem in session logic could lead to the SMTP service crashing (OpenBSD 6.0 errata 010)
- Avoid falling back to a weak digest for (EC)DH with using SNI with TLS library (OpenBSD 6.0 errata 009)
- Avoid unbounded memory growth in TLS library that could be triggered by a TLS client repeatedly renegotiating and sending OCSP Status Request TLS extensions (OpenBSD 6.0 errata 008)

- Revert a change that adds additional cleaning of EVP cipher contexts as some software relied on the old behaviour (OpenBSD 6.0 errata 007)
- During parsing of the IKEv2 service configuration Pre-Shared key authentication was mistakenly disabled (OpenBSD 6.0 errata 006)
- Limit the number of wscons fonts that can be loaded into the kernel (OpenBSD 6.0 errata 005)
- A logic issue in the mail service's header parsing could cause SMTP sessions to hang (OpenBSD 6.0 errata 004)
- Improve parsing of Host-header by following RFC 7230 Section 5.4 more closely (OpenBSD 6.0 errata 003)
- Revert incorrect version bumps in Perl modules (OpenBSD 6.0 errata 002)
- Missing overflow checks in the kernel's virtual memory subsystem could lead to panics (OpenBSD 6.0 errata 001)