

Release Notes

TNOS® 3.1.11

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

TNOS® 3.1.11
Release Notes

June 2017

Esdenera and TNOS are registered trademarks of Esdenera Networks GmbH.

doc 1c144e49663ba6016a0ec4fd07d4bbd497af6caa

Contents

3.1.11 Release Notes	3
Release History	3
Enhancements	3
Fixes	4

3.1.11 Release Notes

Release History

Version	Release Date
3.1.11	2017-06-14
3.1.10	2017-06-13
3.1.09	2017-05-31
3.1.08	2017-05-26
3.1.07	2017-05-24
3.1.06	2017-05-19
3.1.05	2017-05-12
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

3.1.11

- **system upgrade** now defaults to the latest image if no URL is specified

3.1.10

- **system ssh authenticationmethods** has been added, allowing configurations where multiple authentication methods are required before a user is granted SSH access to the system

3.1.08

- Disk layout for new installs has changed to meet Microsoft's requirements for Azure images

3.1.07

- Allow licenses to be granted for KVM based virtual machines

3.1.05

- Initial release for Microsoft Azure Marketplace

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

3.1.11

- The driver for the Xen Blkfront paravirtual storage interface now handles 64KB transfers

3.1.10

- Accept multiple IKEv2 rules as a valid configuration
- An unprivileged user with access to the console could crash the system (OpenBSD 6.0 errata 028)
- Avoid a race condition in File::Path Perl module (OpenBSD 6.0 errata 026)

3.1.09

- A problem which caused `crypto ca` commands to fail has been corrected

3.1.07

- A problem creating new certificate revocations in the CLI has been resolved
- The kernel could leak memory when processing ICMP packets with IP options. These packets are blocked by default (OpenBSD 6.0 errata 025)

3.1.06

- Add a gap of 1MB between the stack and mmap spaces (OpenBSD 6.0 errata 024)

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 infinite 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)