OpenXT 9.0.0 Release

Table of Contents

1. Platform

1.1. Introduction

These are the Release Notes for the 9.0.0 release of OpenXT. The 9.0.0 release strives to modernize OpenXT and align many of its core components with upstream. For example, 9.0.0 is shipping with:

- Xen 4.12 and Linux LTS 4.19
- "Argo", the successor to v4v
- 64-bit dom0 and service vms
- upstream blktap3
- Initial support for HVM UEFI Guests
- SRTM+DRTM for Host UEFI installs

In future releases, the OpenXT Maintainers and Contributors hope to build upon this foundation of modernization, offering new features, and continuing to align with modern, upstream software packages.

Finally, thank you to everyone in the community who contributed to the 9.0.0 release, it wouldn't have been possible without your hard work and dedication.

1.2. OE Layers and Core Component Versions

The 9.0.0 release is a tagged checkpoint of the stable-9 branch.

- OpenEmbedded: Pyro
  - openembedded-core: 819aa151bd build-appliance-image: Update to pyro head revision
  - meta-openembedded: 9eaebc6e7 wireshark: Update Package to 2.2.12
  - meta-intel: df4b25bcd linux-intel/4.9: update to 4.9.116
  - meta-java: 0c27b12 icedtea-native: Fix segmentation build during build
  - meta-selinux: b1dac7e policycorutils: package files in base_sbindir.
  - meta-virtualization: e3402d9 seabios: update SRC_URI to: https://www.seabios.org/downloads/
- Xen: 4.12.1-pre
  - xen: b4f291b xl: handle PVH type in apply_global_affinity_masks again
- Linux kernels: 4.19.53
  - linux 9f31eb6 Linux 4.19.53

1.3. Measurement support

OpenXT supports two modes of measurement. Each mode is enforced automatically depending on the boot method of the OpenXT installation (Legacy vs UEFI).

As for Legacy or UEFI support, it is not currently possible to transistion or upgrade an existing OpenXT installation from Legacy to UEFI, therefore it is not possible to change an existing measurement scheme or forward seal against a different one.

Legacy boot

Legacy installation will perform DRTM measurement using TBoot. It requires a compatible TPM chip and TXT to be enabled in the BIOS before installing OpenXT.

UEFI

UEFI installation will perform SRTM+DRTM measurement. It requires a compatible TPM chip and TXT to be enabled in the BIOS before installing OpenXT.

1.4. Package upgrades: Dom0

- atapi-pt-helper: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- audio-helper: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- blktap3: 0+git0+4c8e89be4e-r0 → 0+git0+a7832564b4-r0
- compleat: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- curl: 7.54.0-r0 → 7.65.1-r0
- dbd: git-r0 → 0+git0+eec9ec9068-r0
- dialog: 1.2-20150225-r0 → 1.3-20160828-r0
- dm-agent: 0+git0+ccfca235de-r0 → none
- drm-surfman-plugin: 0+git0+3263678cd1-r0 → 0+git0+f972c2d33e-r0
- fbtap: 0+git0+c81549a8f4-r0 → 0+git0+2edd6c7ae1-r0
- heimdallr: git-r0 → 0+git0+16b0da1e69-r0
- intel-microcode: 20180807-r0 → 20190514a-r0
- iproute2: 4.10.0-r0.2 → 4.10.0-r0
- kernel: 4.14.66-r0 → 4.19.53-r0
- libcurl4: 7.54.0-r0 → 7.65.1-r0
- libdmbus-0.1-1: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- libicbinn-1.0-0: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libicbinn-1.0-server: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libidn: 1.33-r0 → 2.2.0-r0
- libpci3: 3.5.2-r0 → 3.5.2-r0.1
- libsapi0: git.0+56fec897d5-r0 → none
- libsndfile1: 1.0.27-r0 → 1.0.28-r0
- libsqlite3-0: 3:3.17.0-r0 → 3:3.29.0-r0
- libsurfman-2.1-0: 0+git0+3263678cd1-r0 → 0+git0+f972c2d33e-r0

- libtcti: git.0+56fec897d5-r0 → none
- libtirpc: 1.0.2-r0 → 1.1.4-r0
- libv4v: git0+c0c98489b4-r0 → none
- libxch-rpc: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- libxchdb: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- libxchutils: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- libxchv4v: 0+git0+c47783e944-r0 → none
- libxchwebsocket: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- libxchxenstore: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- libxcxenstore: 0+git0+c47783e944-r1 → 0+git0+27af244d20-r1
- libxencall1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxenctrl4.9: 4.9.3-r0 → none
- libxendevicemodel1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxenevtchn1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxenforeignmemory1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxengnttab1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxenguest4.9: 4.9.3-r0 → none
- libxenlight4.9: 4.9.3-r0 → none
- libxenmgr-core: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- libxenstat0: 4.9.3-r0 → none
- libxenstore3.0: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxentoollog1: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxlutil4.9: 4.9.3-r0 → none
- linux-firmware: 1:0.0+git0+6f5257c629-r0 → 1:0.0+git0+7bc2464513-r0
- linuxfb-surfman-plugin: 0+git0+3263678cd1-r0 → 0+git0+f972c2d33e-r0
- modules: 1.0-r1 → none
- nss: 3.34.1-r0 → 3.45-r0
- pciutils: 3.5.2-r0 → 3.5.2-r0.1
- qemu-dm: 2.6.2-r17.6 → 3.1.0-r17.6
- qmp-helper: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- rpc-proxy: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- rpcbind: 0.2.4-r0 → none
- shim: 14+git0+3ad44002b7-r0 → 14+git0+6c8d08c0af-r0
- surfman: 0+git0+3263678cd1-r0 → 0+git0+f972c2d33e-r0
- tboot: 1.9.6-r0 → 1.9.9-r0

- tpm2-tools: git.0+33cd0d966f-r0 → 3.1.3-r0
- udbus: 0+git0+c47783e944-r0 → 0+git0+27af244d20-r0
- uid: git-r0 → 0+git0+85bdfe0334-r0
- updatemgr: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- upgrade-db: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- v4v-module: git0+c0c98489b4-r0 → none
- vusb-daemon: 0+git0+f0275111fc-r0 → 0+git0+873765e2d4-r0
- wget: 1.19.1-r0 → 1.19.2-r0
- xcpmd: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- xec: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- xen: 4.9.3+git0+85af12d841-r0 → RELEASE-4.12.0+git0+41658b5c44-r0
- xenclient-feed-configs: 1909-r15 → 6676-r15
- xenclient-input-daemon: 0+git0+081e565e74-r0 → 0+git0+b67f92fd99-r0
- xenclient-nwd: 0+git0+6ee8cc614b-r0 → 0+git0+35376b1438-r0
- xenclient-toolstack: 0+git0+7702618789-r0 → 0+git0+a5ca565cb6-r0
- xenmgr: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- xenmgr-data: 0+git0+b0490a4aa5-r0 → 0+git0+faf5aaabfc-r0
- argo-module: none → git0+2bb6f34f92-r0
- ipxe: none → gitr0+827dd1bfee-r0
- libargo: none → git0+2bb6f34f92-r0
- libargo-bin: none → git0+2bb6f34f92-r0
- libxchargo: none → 0+git0+27af244d20-r0
- libxenctrl4.12: none → RELEASE-4.12.0-r0
- libxenguest4.12: none → RELEASE-4.12.0-r0
- libxenlight4.12: none → RELEASE-4.12.0-r0
- libxenstat4.12: none → RELEASE-4.12.0-r0
- libxentoolcore1: none → RELEASE-4.12.0-r0
- libxlutil4.12: none → RELEASE-4.12.0-r0
- modules-dom0: none → 1.0-r1.1
- ovmf: none → git-r0
- rsyslog-conf-dom0: none → 1.0-r0
- tpm2-tss: none → 2.0.0-r0
- txt-info-module: none → 1.0-r0

1.5. Package upgrades: UIVM

- aspell: 0.60.6.1-r1 → none
- enchant: 1.6.0-r3 → none
- iproute2: 4.10.0-r0.2 → 4.10.0-r0
- kernel: 4.14.66-r0 → 4.19.53-r0
- libaspell15: 0.60.6.1-r1 → none
- libdrm: 2.4.75-r0 → none
- libepoxy0: 1.4.0-r0 → none
- libgl-mesa: 2:17.0.2-r0 → none
- libglapi0: 2:17.0.2-r0 → none
- libicbinn-1.0-0: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libicbinn-1.0-client: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libpci3: 3.5.2-r0 → 3.5.2-r0.1
- libsm6: 1:1.2.2-r0.1 → 1:1.2.2-r0
- libsndfile1: 1.0.27-r0 → 1.0.28-r0
- libsqlite3-0: 3:3.17.0-r0 → 3:3.29.0-r0
- libtirpc: 1.0.2-r0 → 1.1.4-r0
- libv4v: git0+c0c98489b4-r0 → none
- libxenstore3.0: 4.9.3-r0 → RELEASE-4.12.0-r0
- libxfont1: 1:1.5.2-r0 → none
- libxi6: 1:1.4.5-r0 → 1:1.7.9-r0
- libxklavier16: 5.0-r0.1 → 5.4-r0
- libxrandr2: 1:1.3.2-r0 → 1:1.5.1-r0
- libxxf86vm1: 1:1.1.4-r0 → none
- mesa-megadriver: 2:17.0.2-r0 → none
- modules: 1.0-r1 → none
- pciutils: 3.5.2-r0 → 3.5.2-r0.1
- rpcbind: 0.2.4-r0 → none
- v4v-module: git0+c0c98489b4-r0 → none
- xdotool: 2.20100818.3004-r0 → none
- xen: 4.9.3-r0 → RELEASE-4.12.0-r0
- xenclient-feed-configs: 1909-r15 → 6676-r15
- xenfb2: 0+git0+fad222619c-r0 → 0+git0+1c1275efa9-r0
- xf86-input-evdev: 2:2.6.0-r17.0 → 2:2.10.5-r0

- xf86-input-keyboard: 2:1.6.1-r17.0 → 2:1.9.0-r0
- xf86-input-mouse: 2:1.7.1-r17.0 → 2:1.9.2-r0
- xf86-video-fbdev: 2:0.4.2-r17.0.1 → 2:0.4.4-r0
- xkeyboard-config: 1.4-r4 → 2.20-r0
- xrandr: 1:1.3.5-r1 → 1:1.5.0-r0
- xserver-xf86-config: 0.1-r33.1 → 0.1-r33
- xserver-xorg: 2:1.11.2-r1.2 → 2:1.19.5-r0
- argo-module: none → git0+2bb6f34f92-r0
- iso-codes: none → 3.74-r0
- libargo: none → git0+2bb6f34f92-r0
- libargo-bin: none → git0+2bb6f34f92-r0
- libevdev: none → 1.5.6-r0
- libinput: none → 1.6.1-r0
- libxentoolcore1: none → RELEASE-4.12.0-r0
- libxfont2-2: none → 2.0.1-r0
- modules-uivm: none → 1.0-r1.1
- mtdev: none → 1.1.5-r0
- rsyslog-conf: none → 8.22.0-r0
- xf86-input-libinput: none → 2:0.24.0-r0

1.6. Package upgrades: NDVM (Network)

- carrier-detect: 0+git0+916b9bfc35-r0 → 0+git0+b29a2fd833-r0
- db-tools: 0+git0+08ef5856d8-r0 → 0+git0+eec9ec9068-r0
- iproute2: 4.10.0-r0.2 → 4.10.0-r0
- kernel: 4.14.66-r0 → 4.19.53-r0
- libicbinn-1.0-0: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libicbinn-1.0-client: 0+git0+760f5b3553-r0 → 0+git0+00e4535ebd-r0
- libpci3: 3.5.2-r0 → 3.5.2-r0.1
- libtirpc: 1.0.2-r0 → 1.1.4-r0
- libv4v: git0+c0c98489b4-r0 → none
- libxenstore3.0: 4.9.3-r0 → RELEASE-4.12.0-r0
- linux-firmware: 1:0.0+git0+6f5257c629-r0 → 1:0.0+git0+7bc2464513-r0
- modules: 1.0-r1 → none
- pciutils: 3.5.2-r0 → 3.5.2-r0.1
- rpcbind: 0.2.4-r0 → none

- v4v-module: git0+c0c98489b4-r0 → none
- wget: 1.19.1-r0 → 1.19.2-r0
- xen: 4.9.3-r0 → RELEASE-4.12.0-r0
- xenclient-feed-configs: 1909-r15 → 6676-r15
- xenclient-nws: 0+git0+6ee8cc614b-r0 → 0+git0+35376b1438-r0
- xenclient-toolstack: 0+git0+7702618789-r0 → 0+git0+a5ca565cb6-r0
- argo-module: none → git0+2bb6f34f92-r0
- libargo: none → git0+2bb6f34f92-r0
- libargo-bin: none → git0+2bb6f34f92-r0
- libxentoolcore1: none → RELEASE-4.12.0-r0
- modules-ndvm: none → 1.0-r1.1
- rsyslog-conf: none → 8.22.0-r0

2. Feature Additions

- xenclient-oe/f2bc86ed: xterm: Enable TrueType fonts, OXT-1509
- xenclient-oe/ada91543: xsessionconfig: Use monospace font for xterm, OXT-1509
- idl/ba021902: idl: Add VirtType to support PVH, OXT-1383
- input/2f546c8b: input: Handle PVHv2 like PV guests., OXT-1648
- manager/04ca4c24: Fix XL VM config files for Xen 4.10, OXT-1277
- manager/f638523f: xenmgr: Add nogfx support, OXT-1327
- manager/ed4632a2: xenmgr: Remove unused data type, OXT-1327
- manager/bdf5bd02: PartTable: Fix for new fdisk, OXT-1327
- manager/f87cfe1d: xenmgr: Remove enumServiceVmTemplates, OXT-1327
- manager/8e3a80b9: xenmgr: Select ndvm pv/hvm mode at runtime, OXT-1327
- manager/1bfa5096: templates: Update ndvm for partitioned disk image, OXT-1327
- manager/519cfa7d: templates: Rename pv ndvm templates, OXT-1327
- manager/2050e911: templates: Add hvm ndvm templates, OXT-1327
- manager/f6bc127d: xenmgr: Honor /xenmgr/overwrite-ndvm-settings, OXT-1327
- manager/c02ee587: upgrade-db: Migration for partitioned disk ndvm, OXT-1327
- manager/58aa0ffa: upgrade-db: Syncvm flask label migration, OXT-1384
- manager/ccc7c79e: xenmgr: Add VirtType, OXT-1383
- manager/a095b596: xenmgr: Remove use of vmHvm, OXT-1383
- manager/61f44113: xenmgr: Remove get/setVmHvm, OXT-1383
- manager/671b1bf6: xenmgr: Condition NIC configuration on stubdom && HVM, OXT-1383
- manager/7ef5da23: templates: Convert from hvm to virt-type, OXT-1383
- manager/5ac4c130: Migration 39: Convert hvm to virt-type, OXT-1383
- manager/2cf476cc: xenmgr: Stubdom is only valid for HVM, OXT-1383
- manager/2e0f8df0: xenmgr: getVmStubdom only return True for HVM, OXT-1383
- meta-openxt-ocaml-platform/79d907ca: OXT-1477 : Enable building OCaml binaries for x86_64, OXT-1477
- openxt/dbb3b8b2: Xen: upgrade to 4.10.0, OXT-1277
- openxt/36e031bc: do_build.sh: Copy .disk.vhd images, OXT-1327
- openxt/40b43b98: manifest: Use NDVM partitioned disk image, OXT-1327
- openxt/653690de: build-scripts: Build NDVM partitioned disk images, OXT-1327
- openxt/b32d338c: debian_install.sh: do not fail when /etc/debian_version doesn't exist Debian variants like Devuan may not have that file., OXT-1470
- openxt/a40f33f8: build-scripts: remove architecture info from output files, OXT-1554 OXT-1552

- openxt/ea19daac: [debian] Temporary: Don't install xenmou driver, OXT-1608
- toolstack-data/66d5f9e9: Switch to virt_type for PVH support, OXT-1383
- v4v/e61b83ef: Mark v4v file descriptors read-write, OXT-1304
- v4v/b1dfe102: Add v4v compat ioctl, OXT-1304
- xenclient-oe/a6b1f2fc: Xen: upgrade to 4.10.0, OXT-1277
- xenclient-oe/0a0f654c: openxt_image_types: Add space to _append-ed CONVERSIONTYPES, OXT-1327
- xenclient-oe/a7afc375: openxt_image_types: Remove IMAGE_TYPES appending, OXT-1327
- xenclient-oe/83c48e34: openxt-image-disk: Create partitioned disk image, OXT-1327
- xenclient-oe/f57b4c7e: xenclient-image-common: Inherit openxt-image-disk, OXT-1327
- xenclient-oe/f23ccdf9: Move KERNEL_IMAGETYPE to machine/xenclient-common.conf, OXT-1327
- xenclient-oe/43d5ed71: qemu-dm: Qubes PCI region size rounding, OXT-1327
- xenclient-oe/899d9887: qemu-dm: Avoid segfault in xenmou shutdown, OXT-1327
- xenclient-oe/827c73bc: qemu-dm: Fix surfman-dcl segfault on shutdown, OXT-1327
- xenclient-oe/20d0330e: linux: Update NDVM config for HVM, OXT-1327
- xenclient-oe/2102e1ac: linux: Reduce ndvm kernel defconfig, OXT-1327
- xenclient-oe/c5884d46: base-files: Use xvdb for NDVM swap disk, OXT-1327
- xenclient-oe/8b648b7b: ndvm-image: Switch to using partitioned disk, OXT-1327
- xenclient-oe/8a6df504: initrdscripts: Use xenstore for qemu arguments, OXT-1327
- xenclient-oe/160c33c3: xen-libxl: Drop openxt_qemu_args from stubdom kernel command line, OXT-1327
- xenclient-oe/f80e3283: xen-libxl: Remove unnecessary code change, OXT-1327
- xenclient-oe/1c306c20: xen-libxl: Allow disabling HVM graphics, OXT-1327
- xenclient-oe/8c489150: xen-libxl: Rearrange qemu argument additions, OXT-1327
- xenclient-oe/c3b68bc6: xen-libxl: Conditionalize helper daemons, OXT-1327
- xenclient-oe/b2981e58: xen-libxl: Use a function to fork helpers, OXT-1327
- xenclient-oe/90f4992f: Update create-ndvm for pv/hvm selection, OXT-1327
- xenclient-oe/b2127cb5: qemu-dm: Import qemu-dm-wrapper from dm-agent, OXT-1381
- xenclient-oe/265207d4: initrdscripts: Remove dm-agent from script, OXT-1381
- xenclient-oe/31e984e3: initrdscripts: fix debug log level, OXT-1381
- xenclient-oe/0c00b69a: stubdomain-image: Remove dm-agent, OXT-1381
- xenclient-oe/2a214cfc: packagegroup-dom0: Remove unused dm-agent, OXT-1381
- xenclient-oe/621cde3e: dm-agent: Remove recipe, OXT-1381
- xenclient-oe/52d702c8: refpolicy: Remove dm-agent, OXT-1381

- xenclient-oe/d154c54f: xen: Bypass ACPI SLIC support for PVH, OXT-1383
- xenclient-oe/0dec0d98: refpolicy-mcs: Allow loading signed modules, OXT-1403
- xenclient-oe/3a2060c5: modules-signing: Add basic support for signed modules, OXT-1403
- xenclient-oe/e79d05d5: module-signing: Allow external keys, OXT-1403
- xenclient-oe/88c360b4: linux: dom0 module signing, OXT-1403
- xenclient-oe/929e9721: linux: ndvm module signing, OXT-1403
- xenclient-oe/5eb1f998: linux: uivm module signing, OXT-1403
- xenclient-oe/43ed16a3: linux: stubdom module signing, OXT-1403
- xenclient-oe/2393d816: linux: syncvm module signing, OXT-1403
- xenclient-oe/7dcd42c3: rsyslog: Use custom format for VM messages, OXT-1409
- xenclient-oe/c36e496c: module-signing: Fix SIG_HASH check, OXT-1403
- xenclient-oe/fb3f4c25: module-signing: Find sign-file location at runtime, OXT-1403
- xenclient-oe/74dcc3f4: qemu-dm: implement v4v stream, OXT-1407
- xenclient-oe/42a43df0: qemu-dm: Drop close in chardev-v4v, OXT-1407
- xenclient-oe/08b0b6d3: openxt-ml: Do not mount ESP in seal-system., OXT-1397
- xenclient-oe/bef5c411: Revert "refpolicy-mcs: Allow installer part2 to mount ESP.", OXT-1397
- xenclient-oe/9e8ea326: module-signing: Fix SIGN_FILE error detection, OXT-1403
- xenclient-oe/1b18ae5d: module-signing: Serialize sign_modules with make_scripts, OXT-1403
- xenclient-oe/0325cdd2: libxl: Drop unneeded hunk from libxl-openxt-helpers.patch, OXT-1441
- xenclient-oe/0ef89a5d: libxl: Drop unneeded hunks from libxl-openxt-qemu-args.patch, OXT-1441
- xenclient-oe/457cd98d: Install qemu script as /etc/qemu-ifup, OXT-1441
- xenclient-oe/fcc48fc5: libxl: Drop -boot hunk from libxl-openxt-qemu-args.patch, OXT-1441
- xenclient-oe/f86fcd3b: xen-libxl: Move hunk, OXT-1441
- xenclient-oe/b1941224: libxl: Refresh patch queue, OXT-1441
- xenclient-oe/aa1aea57: lvm udev rules: avoid trying to create bad symlinks lvm expects /dev/mapper to be populated with symlinks, but instead it contains actual blk files. Remove the rule that creates those symlinks., OXT-1274
- xenclient-oe/40b9823b: [tpm2-tools] Uprev from v2.0.0 to v3.1.3, OXT-1456
- xenclient-oe/d977e12b: xorg: Partially restore former configuration., OXT-1463 OXT-1320
- xenclient-oe/b7965c57: qemu-dm: 3.1 uprev, OXT-1499
- xenclient-oe/338c7432: qemu-dm: move PV into qemu-dm.inc, OXT-1499
- xenclient-oe/bc678342: qemu-dm: Refresh patch queue, OXT-1499
- xenclient-oe/729efb49: tpm2-tss: Let OE handle the autoconf., OXT-1485
- xenclient-oe/2fbb5255: tpm2-tss: Simplify tpm2-tss packaging., OXT-1485

- xenclient-oe/e1cd74a0: tpm2-tools: Let OE handle the autoconf., OXT-1485
- xenclient-oe/4a6411b5: xen/xl: Refactor tapdev_is_shared callsites., OXT-1514
- xenclient-oe/efdab5c9: xen/xl: Add pid to syslog() redirections for xl., OXT-1515
- xenclient-oe/b9dfa999: xen/xl: Refactor xenmgr sync for firewall rules., OXT-1516
- xenclient-oe/0476ae9d: [OVMF PXE] Add Intel E1000 binaries to OVMF image, OXT-1439
- xenclient-oe/b3213ed2: shim: switch to upstream + patchqueue This is a first step, which switches to the upstream head that was used for the fork. There shouldn't be any code difference. Next step is to upgrade to v15., OXT-1413
- xenclient-oe/90c6f4a5: OXT-1374: [xen] Remove Kconfig option pv linear-pagetables, OXT-1374
- xenclient-oe/5f6ea20d: kernel: enable cgroups for dom0, OXT-1379
- xenclient-oe/fdaf8be2: [xen] Force synchronous page scrub, OXT-1494
- xenclient-oe/41343e07: [nss] Upgrade nss to 3.45, OXT-1642
- xenclient-oe/08f858d3: [pesign] Cast RHS of macro assignment, OXT-1642
- xenfb2/6b7c1e0a: linux: Deprecated XENFB2_TYPE_UPDATE_FB2M., OXT-1652
- xenfb2/da7d3409: linux: Deprecated XENFB2_TYPE_FB_CACHING., OXT-1652
- xenfb2/eaa590f8: linux: Remove FB2M reset., OXT-1652
- xsm-policy/054f8701: Update base files to Xen 4.10.0, OXT-1277
- xsm-policy/39d08c27: Update policy for Xen 4.10.0, OXT-1277
- xsm-policy/af4665c2: Move HVM self permissions into interface, OXT-1327
- xsm-policy/8f18d71c: Allow NDVM stubdom use, OXT-1327
- xsm-policy/c102040a: [flask] Update for Xen 4.12, OXT-1563 OXT-1550

3. Security Fixes

- xenclient-oe/0dec0d98: refpolicy-mcs: Allow loading signed modules, OXT-1403
- xenclient-oe/3a2060c5: modules-signing: Add basic support for signed modules, OXT-1403
- xenclient-oe/e79d05d5: module-signing: Allow external keys, OXT-1403
- xenclient-oe/88c360b4: linux: dom0 module signing, OXT-1403
- xenclient-oe/929e9721: linux: ndvm module signing, OXT-1403
- xenclient-oe/5eb1f998: linux: uivm module signing, OXT-1403
- xenclient-oe/43ed16a3: linux: stubdom module signing, OXT-1403
- xenclient-oe/2393d816: linux: syncvm module signing, OXT-1403
- xenclient-oe/c36e496c: module-signing: Fix SIG_HASH check, OXT-1403
- xenclient-oe/fb3f4c25: module-signing: Find sign-file location at runtime, OXT-1403
- xenclient-oe/9e8ea326: module-signing: Fix SIGN_FILE error detection, OXT-1403
- xenclient-oe/1b18ae5d: module-signing: Serialize sign_modules with make_scripts, OXT-1403
- xenclient-oe/41343e07: [nss] Upgrade nss to 3.45, OXT-1642
- xenclient-oe/08f858d3: [pesign] Cast RHS of macro assignment, OXT-1642
- xenclient-oe/642e8e94: l1tf: Disable SMT on Xen., OXT-1426
- xenclient-oe/7e15407c: passwd: set all non-root shells to false, OXT-1585 OXT-1586
- openxt/9899a2cb: xen: Move version management to the recipes., OXT-1346
- xenclient-oe/1b88997d: xen: Fetch from git stable branch., OXT-1346
- xenclient-oe/409a525c: xen: upgrade to the tip of stable-4.10., OXT-1425 OXT-1424 OXT-1423 OXT-1343
- xenclient-oe/a71afa5f: [bdwgc] Backport upgrade to bdwgc, OXT-1629
- xenclient-oe/64d5f045: [php] Backport PHP CVE-2017-9120, OXT-1629
- xenclient-oe/c92c63b9: [krb5] Backport krb5 CVE-2017-11462, OXT-1629
- xenclient-oe/a2b61a55: [gnulib] Upgrade to 2017-08-20.18, OXT-1629
- xenclient-oe/3e303969: [libxslt] Backport CVE-2019-11068 fix, OXT-1629
- xenclient-oe/d7a6e010: [python] Backport CVEs for python 2.7, OXT-1629
- xenclient-oe/e021cd4c: [glibc] Backport Critical Glibc CVEs, OXT-1629
- xenclient-oe/6839b9ce: [icu] Backport icu CVE, OXT-1629
- xenclient-oe/2d67c59b: [libsndfile1] Port 1.0.28 from oe-core master, OXT-1629
- xenclient-oe/376c1081: [curl] Upgrade curl to 7.65.1, OXT-1629
- xenclient-oe/d43e719d: [gettext] Backport CVE-2018-18751, OXT-1629
- xenclient-oe/25c49feb: [libxml2] Backport CVE-2017-8872, OXT-1629
- xenclient-oe/4109254f: [elfutils] Backport CVE-2018-16402, OXT-1629

- xenclient-oe/fda0d59e: [busybox] Backport CVE-2017-16544, OXT-1629
- xenclient-oe/394bb8f2: [wget] Upgrade to 1.19.2 for CVEs, OXT-1629
- xenclient-oe/93063ce8: [xserver-xorg] Upgrade to 1.19.5 for CVEs, OXT-1629
- xenclient-oe/1b869c4e: [libpcre] Backport CVE-2017-8786, OXT-1629
- xenclient-oe/403617ed: [sqlite3] Upgrade to 3.20.0 for CVE, OXT-1629
- xenclient-oe/5ee41311: [sqlite3] Upgrade sqlite3 and pseudo, OXT-1629

4. Maintenance Changes

- fbtap/d2080b86: ioctl: FBTAP_IOCGSIZE type width., OXT-1638
- icbinn/6330df81: pyicbinn: Link with -Bsymbolic, OXT-1628
- idl/973a97d5: ahci support: add property *hdtype*, OXT-1123
- input/214da032: [domains] Better filter for dead domains, OXT-1569
- installer/4b69b1a1: Clear outdated files from ESP during upgrades, OXT-1459
- installer/4af6da92: [installer] Only install upgradecompat on upgrades, OXT-1549
- installer/f954959e: seal-system: Run write_config_pcrs from chroot, OXT-1351
- installer/0356eff4: [stable-9] Add boot VGA device warning, OXT-1600
- installer/4844382e: [copy_to_esp] Limit search to target disk only, OXT-1632
- installer/027f5cb4: installer: Handle NVMe symlink aliases., OXT-1654
- installer/fb009ec5: part2: Use common for devnode sanitation., OXT-1654
- manager/64b4682f: xenmgr: remove snapshot disk key on shutdown, OXT-1243
- manager/a5c4077a: xenmgr: Use xl option rtc_timeoffset, OXT-1442
- manager/10c09010: xenmgr: fix nested HVM xl syntax, OXT-1510
- manager/8e7eb2e7: ahci support: update vm templates with appropriate hdtype, OXT-1123
- manager/f38a42c3: fix disk virtual path, OXT-1123
- manager/2eee89b6: ahci support: add xenmgr support to parse *hdtype* config option, OXT-1123
- manager/aa359dab: [xenmgr] Add initrd to xl config, OXT-1287
- manager/aab6bb27: fix iso-hotswap, OXT-1556
- manager/81877da7: xenmgr: Use loopdev for mounting partitions, OXT-1538
- manager/73bb02f3: [xenmgr] Error if VMs disk paths are bad, OXT-1596
- manager/a9faaae4: [linux] Use ide instead of AHCI, OXT-1582
- network/333ae37e: network-slave: Forward 802.1x packets on brbridged, OXT-1437
- openxt/b4dc32d8: Stop using grubx64.efi symlink, OXT-1484
- openxt/4c34e0ce: debian_install.sh: fix install on non-systemd (wheezy) Also fix v4v uninstall., OXT-1348
- openxt/a40f33f8: build-scripts: remove architecture info from output files, OXT-1554 OXT-1552
- openxt/ceb5907d: version: Allow upgrades from 8.0.0., OXT-1611
- pv-linux-drivers/ec8d00c9: v4v: Remove sources from this repository., OXT-251
- surfman/e74cb66f: xenfb2: Amend default framebuffer values., OXT-1639
- surfman/8f36aa78: surfman/drm: Let surfman trigger monitor rescan., OXT-1653
- surfman/1189b086: surfman/drm: Calloc(3) may fail., OXT-1653
- surfman/3a6c89c7: surfman/drm: SEGV connector→modes & upscale limit, OXT-1653

- surfman/4ea6510d: surfman: get_monitor_info() may fail., OXT-1653
- toolstack-data/d485da95: [ui] Disable sleep options, OXT-1589
- toolstack-data/0092bda9: [ui] Disable unused fields in VM Details, OXT-1598
- toolstack-data/b48817bf: [ui] Disable VM and Host Hibernate, OXT-1591
- xenclient-oe/04f6d128: [xl] Use sigsuspend to synch xenmgr and xl domain, OXT-1299
- xenclient-oe/64c3b281: qemu-dm: Remove version from patch directory, OXT-1360
- xenclient-oe/ddbdf0c9: qemu-dm: Use a/b patch format, OXT-1360
- xenclient-oe/df30c41d: qemu-dm: Sort patch hunks, OXT-1360
- xenclient-oe/16f012b6: qemu-dm: Remove unneeded CVE/XSA patches, OXT-1360
- xenclient-oe/ede7177f: qemu-dm: Uprev to 2.12.0, OXT-1360
- xenclient-oe/896a861d: qemu-dm: 2.12 update compile-time-stubdom-flag.patch, OXT-1360
- xenclient-oe/fb42a19d: qemu-dm: 2.12 generic-xenstore-extensions.patch, OXT-1360
- xenclient-oe/e47ac8f2: qemu-dm: 2.12 readonly-ide.patch, OXT-1360
- xenclient-oe/99da42b9: qemu-dm: 2.12 hvm-param-dm-domain.patch, OXT-1360
- xenclient-oe/d9019a8f: qemu-dm: 2.12 logging-syslog.patch, OXT-1360
- xenclient-oe/f9dc42d8: qemu-dm: 2.12 dmbus.patch, OXT-1360
- xenclient-oe/87d783f6: qemu-dm: 2.12 switcher.patch, OXT-1360
- xenclient-oe/f1e99b95: qemu-dm: 2.12 acpi.patch, OXT-1360
- xenclient-oe/715db079: qemu-dm: 2.12 xenmou.patch, OXT-1360
- xenclient-oe/fb5686ed: qemu-dm: 2.12 atapi-pass-through.patch, OXT-1360
- xenclient-oe/d5eb21a0: qemu-dm: 2.12 vbe-xt-extensions.patch, OXT-1360
- xenclient-oe/9f8ae1b1: qemu-dm: 2.12 vga-\{spinlock,shadow-bda}, OXT-1360
- xenclient-oe/d1f80328: qemu-dm: 2.12 surfman-dcl.patch, OXT-1360
- xenclient-oe/b65e76a9: qemu-dm: 2.12 audio-policy.patch, OXT-1360
- xenclient-oe/0b0daca3: qemu-dm: 2.12 msix-cap-disable.patch, OXT-1360
- xenclient-oe/0ce2782c: qemu-dm: 2.12 openxtaudio.patch, OXT-1360
- xenclient-oe/a3b233ff: qemu-dm: 2.12 nic-link-state-propagation.patch, OXT-1360
- xenclient-oe/80329035: qemu-dm: 2.12 acpi-pm-feature.patch, OXT-1360
- xenclient-oe/73c61091: qemu-dm: 2.12 maintain-time-offset.patch, OXT-1360
- xenclient-oe/953488a2: qemu-dm: 2.12 acpi-wakeup.patch, OXT-1360
- xenclient-oe/e41f4646: qemu-dm: 2.12 openxt-misc-fixes.patch, OXT-1360
- xenclient-oe/e5cbac56: qemu-dm: 2.12 qmp-v4v-char-driver.patch, OXT-1360
- xenclient-oe/3e2eca64: qemu-dm: 2.12 use-relative-xenstore-nodes.patch, OXT-1360
- xenclient-oe/2c842afb: qemu-dm: 2.12 exit-mainloop-on-reset.patch, OXT-1360
- xenclient-oe/efe7e7be: qemu-dm: 2.12 write-acpi-state-to-xenstore.patch, OXT-1360

- xenclient-oe/f43f14fe: qemu-dm: 2.12 set-blockdev-ro.patch, OXT-1360
- xenclient-oe/c398b8ae: qemu-dm: 2.12 block-remove-unused-block-format-support.patch, OXT-1360
- xenclient-oe/dad06070: qemu-dm: 2.12 net-Remove-unused-network-options.patch, OXT-1360
- xenclient-oe/79a08367: qemu-dm: Support disabling virtio, OXT-1360
- xenclient-oe/7bd9853e: qemu-dm: Disable TCG, OXT-1360
- xenclient-oe/f6f7b5fe: qemu-dm: Make chardev-v4v more configurable, OXT-1360
- xenclient-oe/b5fbdcda: qemu-dm: Convert and fix switcher keyboard input, OXT-1360
- xenclient-oe/5f38f9bf: qemu-dm: Update readonly-ide.patch, OXT-1360
- xenclient-oe/e83ba694: qemu-dm: Move xen-dmbus to hw/xen/, OXT-1360
- xenclient-oe/c69db3e7: qemu-dm: Drop QEMU_WARN_UNUSED_RESULT hunk, OXT-1360
- xenclient-oe/2ed4eeae: qemu-dm: Avoid segfault in dmbus_send, OXT-1360
- xenclient-oe/c6946d7d: dmidecode: Inherit CC and CFLAGS from OE, OXT-1307
- xenclient-oe/d119f608: linux: 32bit Xen EFI support, OXT-1307
- xenclient-oe/2a1f3ce2: libselinux: Compile with _FILE_OFFSET_BITS=64, OXT-1388
- xenclient-oe/049521c1: xen: Amend xen.efi LoadOptions handling., OXT-1432
- xenclient-oe/52b073b1: xenclient-idl: Add recipe version, OXT-1436
- xenclient-oe/2aa5cbe2: qemu-dm: Forward bridge traffic with group_fwd_mask instead of break_8021d, OXT-1437
- xenclient-oe/5067605b: linux: Remove break-8021d.patch, OXT-1437
- xenclient-oe/9c45fd5c: qemu-dm: 3.0.0 uprev, OXT-1445
- xenclient-oe/9d4c4117: qemu-dm: update hvm-param-dm-domain, OXT-1445
- xenclient-oe/0a4270b3: qemu-dm: update vbe-xt-extenstions, OXT-1445
- xenclient-oe/04375f3f: qemu-dm: update vga-spinlock, OXT-1445
- xenclient-oe/5527d0f2: qemu-dm: update surfman-dcl, OXT-1445
- xenclient-oe/81ebc511: qemu-dm: update audio-policy, OXT-1445
- xenclient-oe/4a3b9183: qemu-dm: update block-remove-unused-block-format-support, OXT-1445
- xenclient-oe/c53f5284: qemu-dm: Refresh patch queue, OXT-1445
- xenclient-oe/c55a4b1c: libxl: Use host_device for stubdom cdrom format, OXT-1445
- xenclient-oe/8a111a5f: qemu-dm: Fix domain focus on reboot for 3.0, OXT-1445
- xenclient-oe/997935c1: oxt-ml: Add seal-system.conf., OXT-1438
- xenclient-oe/642e8e94: l1tf: Disable SMT on Xen., OXT-1426
- xenclient-oe/a57719d5: uefi/tboot: Load microcode from MBI2 modules., OXT-1452
- xenclient-oe/b0633835: grub-efi: Don't create grubx64.efi symlink, OXT-1484

- xenclient-oe/8cbd42e7: fix iso hotswap for linux guests, OXT-1493
- xenclient-oe/fc0f085d: rpc-proxy: initscript: start rpc-proxy even when SELinux is disabled. 2 of the 3 rpc-proxy instances are started with runcon, since we want each process to be in its own SELinux context. However, runcon fails when SELinux is disabled, and rpc-proxy is not started in that case. Fixing this by not running runcon when SELinux is disabled., OXT-1504
- xenclient-oe/c5ffc42f: tboot: Upgrade to 1.9.9, OXT-1446 OXT-1481
- xenclient-oe/9a4d9506: xen/xl: Fix memory fault in libxl create domain., OXT-1517
- xenclient-oe/47a84975: ahci support: provide multiple disk support in case of stubdom, OXT-1123
- xenclient-oe/35bf400a: OXT-1523: Fix auto-generated key signing race, OXT-1523
- xenclient-oe/db72850b: txt_info: TXT resources to user-land., OXT-1506
- xenclient-oe/4d8b7a8e: tboot: Add 0x40f event emulation to pcr-calc., OXT-1506
- xenclient-oe/70d83459: tboot: Add utility to match ACM with platform., OXT-1506
- xenclient-oe/06f84b8f: seal-system: Use event emulation to foward-seal., OXT-1506
- xenclient-oe/88c78c8d: pesign: Set SRCREV to last known-good build., OXT-1532
- xenclient-oe/268deb0d: linux: 4.19.32 micro-upgrade and defconfig cleanup, OXT-1536 OXT-1531
- xenclient-oe/51fa18c5: [xen] Make sure xen Kconfig uses the new TXT_OP, OXT-1541
- xenclient-oe/a8a86932: ml/pcr-calc: Forward sealing from previous version, OXT-1507 OXT-1506 OXT-1540
- xenclient-oe/8077a4f2: ml/pcr-calc: Old eventlog entry handling., OXT-1540
- xenclient-oe/de354ace: [key-functions] Maintain backwards compat, OXT-1547
- xenclient-oe/f2a626a1: [seal-system] Use dd and iflag=direct, OXT-1583
- xenclient-oe/214eeca0: refpolicy: Silence mount AVC, OXT-1538
- xenclient-oe/e4c63f90: refpolicy: Refresh patch queue for mount.te change, OXT-1538
- xenclient-oe/883e1e8c: [upgrade-compat] Include coreutils in the upgrade, OXT-1583
- xenclient-oe/bd250cda: [init] Load i915 driver to accommodate multiple, OXT-1593
- xenclient-oe/96d28534: [xen] Drop hide-cores-from-cpuid.patch, OXT-1574
- xenclient-oe/c8187d74: [libxl] Retry on pci add failure for PT GPU, OXT-1571
- xenclient-oe/72786f2c: keymgmt: Getenforce is not in the installer., OXT-1581
- xenclient-oe/806ae0a5: [stable-9] Enable Radeon and Nouveau kernel modules in installer image, OXT-1600
- xenclient-oe/e8799c61: tpm2: Store pcr configuration in ${tss}.pcrs, OXT-1594
- xenclient-oe/a25fff7d: seal-system: Only import ml-functions, OXT-1594
- xenclient-oe/4fa0cb7d: seal-system: Read pcr selection from /config/config.pcrs, OXT-1594
- xenclient-oe/d9fd0f24: seal-system: Only measure root dev if sealing pcr15, OXT-1594
- xenclient-oe/c8d6abe6: keymanagement: Add tpm-scripts RDEPENDS, OXT-1594

- xenclient-oe/dbf4c959: tpm-scripts: Add tpm\{,2}-tools RDEPENDS, OXT-1594
- xenclient-oe/7e15407c: passwd: set all non-root shells to false, OXT-1585 OXT-1586
- xenclient-oe/37c4d025: base-files: /var/lock → /run/lock, OXT-1565
- xenclient-oe/51098b7e: [xen] Fix argo requeue bugs in upstream Xen, OXT-1617 OXT-1618
- xenclient-oe/eb54ed32: [hvmloader] Pass ipxe ROM to hvmloader, OXT-1627
- xenclient-oe/63c2900a: S9: OXT-1623: libxl: add back stubdom check for helper kill, OXT-1623
- xenclient-oe/55e1312d: S9: OXT-1623: libxl: log error when kill() fails, OXT-1623
- xenclient-oe/4a5abaf0: xinitrc: Create & export XDG_RUNTIME_DIR, OXT-1562
- xenclient-oe/2f98ff84: Uprev libtirpc to 1.1.4, OXT-1628
- xenclient-oe/bd265a91: OXT-1645: console-setup: uprev to 1.192; fixes build, OXT-1645
- xenclient-oe/b37d1592: S9: OXT-1577: udev: fix cdrom eject by disabling locking of cdrom devices, OXT-1577
- xsm-policy/2bf34e6c: [xsm] Add access to resource_map for HVM guests, OXT-1529
- xsm-policy/abf2d4d4: Give dom0 access to mca_op, OXT-1588
- xsm-policy/c102040a: [flask] Update for Xen 4.12, OXT-1563 OXT-1550
- installer/39bcd231: [upgrade] Use the upgrade-compat image, OXT-1539
- manager/dad8f575: templates: Make UIVM default to PVH., OXT-1647
- openxt/9899a2cb: xen: Move version management to the recipes., OXT-1346
- openxt/45c7996c: build-scripts: build new 32-bit upgrade compat image, OXT-1539
- openxt/cb63b910: [upgrade] Add extra image step for update compat, OXT-1539
- surfman/9ca42c12: libsurfman: Use libxc compat foreign interfaces., OXT-1650
- surfman/2c59af55: libsurfman: Translate gpfn→mfn for !PV guests., OXT-1650
- surfman/035ff0f7: libsurfman: Handle PVH cacheattr pinning., OXT-1650
- xenclient-oe/1b88997d: xen: Fetch from git stable branch., OXT-1346
- xenclient-oe/b12067ac: dmidecode: bbappend upstream recipe., OXT-1408
- xenclient-oe/feb98758: linux: micro upgrade to 4.14.63, OXT-1415
- xenclient-oe/409a525c: xen: upgrade to the tip of stable-4.10., OXT-1425 OXT-1424 OXT-1423 OXT-1343
- xenclient-oe/ac6eeb29: recipes-graphics: Remove xorg ducplicate recipes., OXT-1463
- xenclient-oe/efc108bf: uivm: Cleanup uivm image/machine conf., OXT-1463
- xenclient-oe/ead04c57: fbdev: Add back randr1.2 patch for fb resizing., OXT-1463
- xenclient-oe/e9e79367: xdotool: Retire recipe., OXT-1463
- xenclient-oe/d977e12b: xorg: Partially restore former configuration., OXT-1463 OXT-1320
- xenclient-oe/f98ae6dd: seal-system: Update evtlog overrides, OXT-1481
- xenclient-oe/66e67f78: tboot: Use lcp2_mlehash instead of lcp_mlehash., OXT-1481

- xenclient-oe/29ae9cad: tboot: Remove references to defunct binaries., OXT-1481
- xenclient-oe/b8c7aa55: tboot: Export TCG eventlog to Kernel/VMM., OXT-1507
- xenclient-oe/565ee60f: tboot: Add event-log format to exported data., OXT-1507
- xenclient-oe/fa9e90b0: pcr-calc: Support TPM2.0 TCG agile log., OXT-1507
- xenclient-oe/cb495b13: [upgrade] Build new 32-bit compat image to support, OXT-1539
- xenclient-oe/e207bd08: pcr-calc: Fix path to legacy event-log., OXT-1507
- xenclient-oe/f40892cc: [xen] Uprev from 4.11 to 4.12, OXT-1454 OXT-1604
- xenclient-oe/b5104bfa: [xen] Port argo implementation of viptables, OXT-1502
- xenclient-oe/a1d1a02f: [linux] Upgrade from 4.19.44 to 4.19.53, OXT-1630
- xenclient-oe/5aa90010: ovmf: Amend sha256sum for PREBOOT.EXE 24.1, OXT-1633
- xenclient-oe/a71afa5f: [bdwgc] Backport upgrade to bdwgc, OXT-1629
- xenclient-oe/64d5f045: [php] Backport PHP CVE-2017-9120, OXT-1629
- xenclient-oe/c92c63b9: [krb5] Backport krb5 CVE-2017-11462, OXT-1629
- xenclient-oe/a2b61a55: [gnulib] Upgrade to 2017-08-20.18, OXT-1629
- xenclient-oe/3e303969: [libxslt] Backport CVE-2019-11068 fix, OXT-1629
- xenclient-oe/d7a6e010: [python] Backport CVEs for python 2.7, OXT-1629
- xenclient-oe/e021cd4c: [glibc] Backport Critical Glibc CVEs, OXT-1629
- xenclient-oe/6839b9ce: [icu] Backport icu CVE, OXT-1629
- xenclient-oe/2d67c59b: [libsndfile1] Port 1.0.28 from oe-core master, OXT-1629
- xenclient-oe/376c1081: [curl] Upgrade curl to 7.65.1, OXT-1629
- xenclient-oe/d43e719d: [gettext] Backport CVE-2018-18751, OXT-1629
- xenclient-oe/25c49feb: [libxml2] Backport CVE-2017-8872, OXT-1629
- xenclient-oe/4109254f: [elfutils] Backport CVE-2018-16402, OXT-1629
- xenclient-oe/fda0d59e: [busybox] Backport CVE-2017-16544, OXT-1629
- xenclient-oe/394bb8f2: [wget] Upgrade to 1.19.2 for CVEs, OXT-1629
- xenclient-oe/93063ce8: [xserver-xorg] Upgrade to 1.19.5 for CVEs, OXT-1629
- xenclient-oe/1b869c4e: [libpcre] Backport CVE-2017-8786, OXT-1629
- xenclient-oe/403617ed: [sqlite3] Upgrade to 3.20.0 for CVE, OXT-1629
- xenclient-oe/fb9401ef: S9 : OXT-1636 : libnl : fix disabling of network, OXT-1636
- xenclient-oe/5ee41311: [sqlite3] Upgrade sqlite3 and pseudo, OXT-1629
- xenclient-oe/cdd20edf: linux: Add PVH support config for UIVM., OXT-1649
- xenfb2/47e8a8fa: linux: Xenfb2 intialisation conditions., OXT-1651
- icbinn/46cd1e58: [argo] Replace v4v with argo, OXT-1464
- idl/c46f742e: [argo] Replace v4v with argo, OXT-1464
- input/86e5109f: [argo] Replace v4v with argo, OXT-1464

- manager/8a8e9b34: [argo] Replace v4v with argo, OXT-1464
- network/8d684c65: [argo] Replace v4v with argo, OXT-1464
- openxt/1fe57281: example-config: Reset repos and tags for upstream pyro, OXT-880
- surfman/03d811ce: [argo] Replace v4v with argo, OXT-1464
- v4v/9a925814: [xen] Bring macros in line with Xen 4.12, OXT-1454
- vusb-daemon/d0582b0c: [argo] Replace v4v with argo, OXT-1464
- xclibs/a009d88c: [argo] Replace v4v with argo, OXT-1464
- xctools/7e4a54b2: [argo] Replace v4v with argo, OXT-1464
- xenclient-oe/3ecc0c5f: switch to upstream blktap3, OXT-1474
- xenclient-oe/feff5a53: xen: upgrade to 4.11, OXT-1454
- xenclient-oe/156dfbf0: OXT-1476: xen: remove hardcoded target arch in recipes, OXT-1476
- xenclient-oe/ab84e1eb: [xen] Temporarily use v4v in place of Argo, OXT-1454
- xenclient-oe/c226fcf9: [v4v] Remove recipes and replace with argo, OXT-1464
- xenclient-oe/b0ec735b: [kernel] Replace v4v with argo, OXT-1464
- xenclient-oe/0781a70c: [xen] Replace v4v with argo, OXT-1464
- xenclient-oe/c3ede3ab: [xen] Add argo-suppress-debug-messages.patch, OXT-1464
- xenclient-oe/a0b37112: [qemu] Replace v4v with argo, OXT-1464
- xenclient-oe/113e4db1: [dom0] Replace v4v with argo, OXT-1464
- xenclient-oe/8dd86aec: [uivm] Replace v4v with argo, OXT-1464
- xenclient-oe/b553b1df: [ndvm] Replace v4v with argo, OXT-1464
- xenclient-oe/1717f716: [syncvm] Replace v4v with argo, OXT-1464
- xenclient-oe/d9070438: [selinux] Replace v4v with argo, OXT-1464
- xenclient-oe/aab7299e: [OE images] Replace v4v with argo, OXT-1464
- xsm-policy/3949dc2c: [argo] Replace v4v with argo, OXT-1464
- xsm-policy/7fdf2907: [argo] Add new flask rules, OXT-1464
- fbtap/67520bf1: git: Add gitignore.
- idl/b656f066: Added Bios option to xenmgr interfaces
- input/a675f6bd: input: Potential overflow.
- input/61677f0a: input: Fallthrough statements.o
- input/e93e3959: input: Libevent 2.x changes.
- input/0e3c1446: Adjust for 64 bits
- input/f2e5f19a: Add missing 64 bits adjustment
- input/92e46258: [switcher] Replace macro with individual functions
- installer/4e6f6eca: Install tboot and sinit modules to ESP
- installer/900047d6: [upgrade] Don’t attempt to claim the TPM if upgrading

- installer/316ee828: [tpm2-tools] Uprev from v2.0.0 to v3.1.3
- installer/7c105d2c: part2: Add support for gunzip-ing files
- installer/c57e6b24: install-main: Return failure from create_lv
- installer/9ce5db86: install-main: Add do_cmd to seal_system
- installer/85c3240d: install-main: Report mount_upgrade_compat failures
- installer/29a969cd: Updates based on Eric's comments
- installer/3cac2d9e: Update based on Jean's comment
- installer/cf68a04e: Fix a typo in user facing message
- manager/c1fc2e22: xec-vm: fix suspend/resume to/from file
- manager/d50bcc5b: Add BIOS option for guest config
- manager/02aea253: xenmgr: Remove unused stubdom settings
- manager/c7137eb1: xenmgr: Remove mountOffset & readPartTable
- manager/ca840644: xenmgr: Throw error for invalid partitions
- manager/e5531581: rpc-proxy: Lower verbosity
- manager/9a8ab990: xenmgr: Print the uuid during state checks
- manager/6f624116: rpc-proxy: Lower EOF verbosity level
- manager/8e935075: xenmgr: Only pass --partscan when expecting a partition
- manager/b16cb801: xenmgr: Reconnect VIFs manually
- manager/f276b397: xenmgr: Use /dev/hvc0 for measurement failure messages
- manager/9962de9e: xenmgr: avoid leaking FDs to run scripts
- manager/dde33eec: xenmgr: Fix Power control affects VM and Host
- manager/99377bc6: xenmgr: Add xl trigger power to HVM shutdown
- manager/33b2d25b: xenmgr: Close some FD leaks
- manager/509819a0: [xenmgr] Default to hvm ndvm for x64
- meta-openxt-haskell-platform/1c9f4c41: [ghc] Include upstream patches for x64 support
- meta-openxt-haskell-platform/de80ecdc: ghc: add yet another segv fix
- network/f07e0bb8: dnsmasq-script: Use db-rm-dom0
- openxt/be766ad8: oe-core: Use tip of pyro.
- openxt/c5f455d3: stable-8 is branched, bump master version to 9
- openxt/ca7b17c8: Revert "STABLE-8: openxt: Use fixed revisions for stable branch."
- openxt/518f8d85: example-config: Add meta-openxt- tags
- openxt/2d51d328: example-config: Use git submodules by default
- openxt/e63c1217: oe/setup.sh: Create .quiltrc in OE build container
- openxt/3ff7815c: Add build script support for Ubuntu 18.04
- openxt/ff333173: Add forward compatibility for lxc configs

- openxt/6dd4b0d0: Address comments in PR #322
- openxt/73218f84: debian install script: ensure current kernel headers are installed The kernel headers are automatically installed as a dkms dependency. However, apt will install the headers for the latest kernel, which is not necessarily the current kernel, especially if the user didn't dist-upgrade as recommended.
- openxt/0b7568c2: build-scripts: reverse build order OE takes 3 hours to build, Centos Debian and Windows each take about 5 minutes. However, those last 3 are about as likely to fail as OE, maybe even more so for Windows. In an attempt to fail as fast as possible, build:
- Windows first, that randomly breaks, especially around monthly updates
- Centos second, since the container tends to fail to start after builder reboots
- Debian third, less likely to break but really quick
- OE last, since it's the longest step
- openxt/31c25524: Fix librpmbuild package name
- openxt/850f00be: meta-selinux: freeze layer to latest safe commit The meta-selinux layer doesn't have a pyro branch, so we were following master. But master aligns with the OE/Yocto master branches, not pyro. As master diverges, the probability of new changes breaking OpenXT increases. This is what just happened. This freezes the layer to prevent that from happening again.
- openxt/5e1d2a93: build-scripts: switch to 64 bits
- openxt/105c887b: build-scripts: add symlink in OE rootfs to fix the build
- openxt/95f190ef: build-scripts: manifest: add upgrade-compat
- openxt/9fb23796: Freeze all remote layers in stable-9
- openxt/975579ed: Allow upgrade from 8.0.1 and 8.0.2 to 9.0.0, at least for now
- openxt/ebbae353: do_build: Remove sysroot
- openxt/050f5d14: do_build: Allow options to override .config
- openxt/a816b8f0: do_build: Print date and time at completion
- openxt/e0c483ea: build-scripts: linux install: skip the v4v packages Build and ship them but don't install them by default, since OpenXT uses argo now. They can still be installed manually with apt-get/yum if needed.
- pv-linux-drivers/8c2ad728: openxt-vusb: Add timeout to device teardown
- pv-linux-drivers/b249e32f: openxt-vusb: fix for Linux 4.19
- surfman/46810bd6: drm: Initialize offset with psurface.
- surfman/356b9231: drm: Amend printf format.
- surfman/2684b2ea: surfman/drm: Makefile dependencies.
- surfman/69f61462: surfman: xc_domain_getinfo usage.
- sync-client/78fad452: Convert from v4v to argo
- toolstack-data/9cf8b11a: Added BIOS option to UI
- toolstack-data/ceb3d7eb: Rename SeaBIOS to Legacy in option menu

- v4v/843a7fda: Rebase v4v on 4.19
- vusb-daemon/d016da73: Use 1 select() call and let it block
- xc-windows/fb5e26fa: Remove disk-related drivers from the build
- xclibs/03e0832e: [xclibs] Make sure foreign calls use 64 types
- xctools/ad4dff17: xcpmd: snprintf truncation warnings.
- xctools/fdb48611: xcpmd: libevent2 macro conflict.
- xctools/838e57b6: Adjust for 64 bits
- xctools/2026cbb5: [audio_helper] Remove "Dates Modified" section
- xenclient-oe/abad3bec: rsync: PACKAGECONFIG is attr not xattr.
- xenclient-oe/a98a4ee6: xorg-lib: libxrandr configure options.
- xenclient-oe/07c91619: xorg-drivers: Silence QA warnings.
- xenclient-oe/ef446353: refpolicy: fix some tapdisk AVCs
- xenclient-oe/bcc5d5c6: Update Xen patches: support for SecureBoot and minor fixes
- xenclient-oe/477e393e: Xen 4.10: remove unused patches and incorrect comment
- xenclient-oe/3fc95186: Xen 4.10: attempt at fixing xen-translate.patch
- xenclient-oe/14d95f04: libxl: fix save by allowing vNUMA-enabled guests to be saved
- xenclient-oe/ed442a76: linux: Remove Remote Control & Infrared drivers
- xenclient-oe/79f97bc8: xenclient-installer: Make package arch-independent
- xenclient-oe/fcbc5ba2: e2fsprogs: fork a meta-selinux patch meta-selinux doesn't have a pyro branch, so we track its master branch. However, openembedded-core updated e2fsprogs (to 1.44.3) in master. So meta-selinux updated their e2fsprogs patches, and one of them doesn't apply to e2fsprogs 1.43.4 anymore, so this commit forks it. This is not ideal, but it's that or freezing meta-selinux. (or convince them to start maintaining a pyro branch)
- xenclient-oe/b73b0837: openxt-ml: Add usage to seal-system.
- xenclient-oe/f93c436f: Launch tboot from Xen.efi
- xenclient-oe/fdaa3dcc: dom0: disable auto-loading of a couple modules dom0 doesn't provide network backends in OpenXT, ndvm does, so xen-netback is not needed. The wacom module isn't even built for dom0.
- xenclient-oe/4c8e4e99: Fix-up ovmf recipe to force 64-bit and install the bin Xen needs
- xenclient-oe/281956b6: xen: Patch-queue initial refresh.
- xenclient-oe/77f07da7: xen: Package xen-diag.
- xenclient-oe/4a2d14ff: syncvm: Specify read-only-rootfs IMAGE_FEATURES
- xenclient-oe/00c70589: dbd: Add PV variable
- xenclient-oe/b8c5bf5a: uid: Add PV variable
- xenclient-oe/bc70ada4: xenclient-rpcgen:Add PV variable
- xenclient-oe/392f6def: heimdallr: Add PV variable

- xenclient-oe/9fd06a15: libxl: Refresh patch queue
- xenclient-oe/77ab8ace: tboot: Unmask NMI for Xen 4.11 patching.
- xenclient-oe/492de845: installer: remove console=tty2 on the kernel cmdline In the the installer, we don't want the kernel to print anything on screen. The kernel still logs to dmesg and /var/log/kern.log. Additionally, the installer shows /var/log/messages in tty4. With this fix, the installation dialogs should not be disrupted anymore.
- xenclient-oe/ba35765a: openxt-main: Remove nfs from DISTRO_FEATURES
- xenclient-oe/fa05a05f: Removes line that was deleting pkg-config directory/files
- xenclient-oe/867c8eac: openxt_image_types: Fix .vhd size calculation
- xenclient-oe/ba2da6d5: initrdscripts: add openxt framework modules
- xenclient-oe/e2a14f97: dom0-tweaks: change runlevel declaration
- xenclient-oe/ce9431c9: initramfs-image: adopt initramfs-framework init
- xenclient-oe/31ce68fa: openssh: Package openssh-sshd-tcp-init generically
- xenclient-oe/65d38cd7: openssh: RDEPEND on libv4v
- xenclient-oe/942243b8: udev: Delete remnant file
- xenclient-oe/62133985: rsyslog: Remove incorrect logrotate.rsyslog
- xenclient-oe/c0874138: rsyslog: Have openxt-installer use dom0 conf
- xenclient-oe/145787b4: rsyslog: Install a default rsyslog.conf
- xenclient-oe/4cf2173c: Make sure there is buffer control on high memory pages
- xenclient-oe/29a764f0: grub.cfg: sanitize xen console options Remove duplicated statements from the Xen commandline
- xenclient-oe/4d7ec006: linux: Fix domU build of usbback
- xenclient-oe/9318cb0c: [recipes-openxt] remove extra directory depth
- xenclient-oe/df0e95b9: [recipes-openxt] remove script guest-process-stats
- xenclient-oe/82ef124a: [layer] move upstream recipes
- xenclient-oe/ca42ac52: init.root-ro: Remove restorecon /storage
- xenclient-oe/b68bc5b9: rsyslog: Drop klog messages from VMs
- xenclient-oe/09cf303d: rsyslog-conf-dom0: Package dom0 conf
- xenclient-oe/9edbf3d4: rsyslog: Split conf files into seperate subpackage
- xenclient-oe/a5cbc5fd: iproute2: Delete .bbappend
- xenclient-oe/0f46d22e: xen: Remove iproute2 hack
- xenclient-oe/d9e10c78: Add Linux 4.19 support and change the default preference to 4.19
- xenclient-oe/47fe41a0: refpolicy: Fixup audio_helper avcs
- xenclient-oe/4198c492: Use /etc/asound.conf
- xenclient-oe/214b0d78: alsa: Delete .bbappend
- xenclient-oe/4ce01beb: xen-libxl: Re-enable read-only IDE devices

- xenclient-oe/9018f933: xen-libxl: Drop COLO changes from read-only IDE disks
- xenclient-oe/339c1e22: xen-libxl: Patch context updates
- xenclient-oe/100b7b04: Allow xenstored hypercall on Linux 4.19
- xenclient-oe/eb4efd84: module-signing: Handle no module case
- xenclient-oe/f593ba7a: initrd: stubdomain initrd standalone recipe.
- xenclient-oe/32e571a9: libxl: Change libxl-blktap3-do-not-destroy-in-use-tapdevs to tap_list_t
- xenclient-oe/f52432c1: refpolicy: Turn global_ssp on
- xenclient-oe/28d0def7: [network-manager] Fix NM and nm-applet for x64
- xenclient-oe/fe47e426: [linux] Build dom0 and service VM kernels x64
- xenclient-oe/f8dcfa3c: [qemu] Fix compile error for qemu on x64
- xenclient-oe/c11da601: [efi] Turn on efi runtime services in the kernel
- xenclient-oe/87512946: [pciutils] Update the pciutils to support
- xenclient-oe/dc7819ee: [xen] Build 64-bit Xen and the xen pv-shim
- xenclient-oe/ba78ccf9: [webkit] Drop enchant as a dependency
- xenclient-oe/3705dd58: [libtirpc] Compile with fPIC
- xenclient-oe/8c4608f0: svirt-interpose: fix warnings and segfault
- xenclient-oe/67c06bbc: rsyslog: Fix broken packaging
- xenclient-oe/ad3065ae: rsyslog-conf-dom0: Fix RPROVIDES
- xenclient-oe/c33eeed6: linux-firmware: update to latest rev
- xenclient-oe/ba1c20c1: openxt-main: Add PREFERRED_RPROVIDER_rsyslog-conf
- xenclient-oe/184460ed: installer: bump rootfs size to accomodate new firmwares
- xenclient-oe/02f176cf: Update 4.19 Kernel for OpenXT to 64-bit
- xenclient-oe/5b3e87b7: tboot: pcr-calc fixes and small refactoring.
- xenclient-oe/d2231a6d: tboot: pcr-calc read event-log from file.
- xenclient-oe/6d4f2389: Update console-setup to 1.188 while also updating the SRC_URI
- xenclient-oe/a7fd0fcc: pcr-calc: Use DEBUG definition from Config.mk.
- xenclient-oe/0cb515b6: logrotate: Amend recipe typos.
- xenclient-oe/21e66e8b: pcr-calc: Futur proof debug macro.
- xenclient-oe/35fffdeb: module-signing: Re-work sign-file selection
- xenclient-oe/60927223: linux: Don’t set tty0 as preferred console for pv.
- xenclient-oe/9640841f: Add tag MULTIBOOT2_TAG_TYPE_EFI64 from Xen EFI to TBOOT
- xenclient-oe/d6633d90: modules: Split into non-machine specific pkgs.
- xenclient-oe/baf6977d: modules-installer: No modules in the image.
- xenclient-oe/9ccb9d03: seal-system: Exit if unable to read rootfs
- xenclient-oe/2162da41: Fix forward seal: Revert "lvm udev rules: avoid trying to create bad

symlinks"

- xenclient-oe/ba8f8804: openxt_image_types: Support ext4 disk images
- xenclient-oe/c40fe9be: Uprev the Linux 4.19 kernel from 4.19.32 to 4.19.44
- xenclient-oe/d6a725c8: Update the intel microcode to 20190312
- xenclient-oe/ec10d239: Add the 20190514a microcode
- xenclient-oe/253272f4: Update the defconfig's for Linux 4.19.44
- xenclient-oe/414c32e6: initscripts: udev-volatiles early script.
- xenclient-oe/cae125a8: Add three KCONFIG grant table patches and a new defconfig
- xenclient-oe/94358934: Revert "[xen] Temporarily use v4v in place of Argo"
- xenclient-oe/84996c16: cgroups: add missing SELinux permissions
- xenclient-oe/2346dfc9: base-files: Fix syncvm fstab & fstab.early
- xenclient-oe/86c7ab38: syncvm: Use /etc/resolv.conf → /var/run/resolv.conf symlink
- xenclient-oe/49d0e4d5: syncvm-tweaks: Define /etc/network/interfaces symlink
- xenclient-oe/c527210c: pyicbinn: RDEPENDS on python-importlib
- xenclient-oe/a6fd6c9d: initscripts: Remove save-rtc.sh
- xenclient-oe/91556a83: Only set rtc for dom0 & installer MACHINE_FEATURES
- xenclient-oe/ab484218: ndvm-image: drop hwclock.sh initscript removal
- xenclient-oe/46e9c192: uivm-image: drop hwclock.sh PACKAGE_REMOVE
- xenclient-oe/20a09d71: oe-addons: Remove unused recipe directory.
- xenclient-oe/9f905f7a: flex: Remove duplicated recipe with upstream.
- xenclient-oe/cbe748f1: python-dbus: Use upstream recipe.
- xenclient-oe/3f236dd2: python-epydoc: Use upstream recipe.
- xenclient-oe/f230002a: libxklavier: Remove local recipe.
- xenclient-oe/07e25ddb: dialog: Remove local recipe.
- xenfb2/5ef3028c: linux: use proper translation function.
- xenfb2/2b9a0495: linux: Refactor shared-page init.
- xenfb2/4fa4b8d0: linux: Remove signed cast on unsigned values.
- xenfb2/6ead473e: linux: align xenfb2_setcolreg on upstream.
- xenfb2/5cee8409: linux: Fix segv in error path.
- xsm-policy/d6439e94: xen 4.10: add missing permissions to set_gnttab_limit
- xsm-policy/d19ae3d5: Enable HVM NDVM
- xsm-policy/bc068e7f: access_vectors: update to Xen 4.11
- xsm-policy/78f99a39: Support Linux 4.19 on Xen 4.11 by adding access to resource_map
- xsm-policy/bd55e0cf: [xsm] x64 flask perms

5. Testing

5.1. Test Criteria

Testing was performed on the stable-9 branch and against several release candidates prior to the OpenxT 9.0.0 release. The following list summarizes publicly disclosed test results.

HVM guests environments

- Windows10 1709 64 bit
- Windows10 1803 64 bit
- Windows10 1809 64 bit
- Ubuntu 18.04 64 bit (note: See Known Issues for Ubuntu for help installing)
- Debian 9.9 (note: See Known Issues for Debian for help installing)
- RHEL 7.5 (note: disable bochs_drm)

Tested platforms

- Dell
  - Dell Optiplex 7040
  - Dell Optiplex 7060
  - Dell Optiplex XE3
  - Dell Latitude E7470
  - Dell Latitude E7490

Tests logs

- General Testcases
- Upgrade and Measurements

6. Known Issues

6.1. QEMU Audio does not work in Windows/Linux VMs

The default emulated audio device is an ac97 device and Windows 7 and later no longer packages an ac97 driver.

The user has two options for audio,

"ac97"
: provides working audio with slight crackling

  - Linux should detect and load ac97 driver.
  - Windows, download and install drivers from Realtek.

"hda"
: provides poor audio quality and severe crackling

  - Linux should detect and load intel_hda driver.
  - Windows automatically installs drivers

To use "hda", you will need to enter the following in Dom0 terminal window,

```
db-write /vm/$( xec-vm -n "<vm name>" get uuid )/config/sound hda
```

- JIRA Issue: OXT-939

6.2. Nvidia Quadro NVS 310, PCI GPU pass-through

Nvidia Quadro NVS 310 GPU passthrough is not supported in OpenXT 9.0.0.

- JIRA Issue: OXT-1070

6.3. Host S3 resume results in a panic early in Xen and reboot

Host S3 is not supported in OpenXT 9.0.0.

- JIRA Issue: OXT-1092

6.4. Host S3 hangs on Broadwell and newer systems

Host S3 is not supported in OpenXT 9.0.0.

- JIRA Issue: OXT-1093

6.5. More than 4 emulated IDE devices cause QEMU to fail to start

OpenXT 9.0.0 limits a VM to a maximum of four emulated IDE devices (CD/DVD/HDD) being attached at one time.

- JIRA Issue: OXT-1123

6.6. Deleting a VM when a USB Device has attached with "Always use with this VM"

If a USB device has been exclusively assigned to a VM and that VM is deleted, then the USB device will no longer be available to assign to another VM.

It is recommended to disconnect any USB devices from a VM before deleting the VM.

- JIRA Issue: OXT-930

6.7. Windows guest intermittently/randomly does not shut down

During testing, it appears that the presence of the "scsifilt.sys" driver can inhibit Windows guests from properly shutting down.

When attempting to shut down a Windows guest and it's state in the UIVM is "On" and not "Shutting Down", then the VM will need to be halted using the "Force Shutdown" option from the VMs menu in the UIVM.

- JIRA Issue: OXT-1240

6.8. Raw disk can no longer be assigned to VMs

OpenXT 9.0.0 does not support RAW disk assignement to HVM guests with stub-domain.

To assign a RAW disk to a guest:

```
xec-vm -n <vm-name> --disk <disk-id> set phys-type phy
xec-vm -n <vm-name> --disk <disk-id> set phys-path <disk-image-path>
```

Then disable the stub-domain:

```
xec-vm -n <vm-name> set stubdom false
```

- JIRA Issue: OXT-1356

6.9. Connected USB storage measured as part of vendor measurements

Some systems will measure the presence of connected USB devices during sealing operation. This will result in measurement failing if the USB device is removed on the next platform reboot. This cannot be worked-around and resealing the platform without the removable media is the only

known option. Firmware updates may be provided by the platform OEM to change this behavior.

- JIRA Issue: OXT-1129

6.10. Blacklisting bochs_drm

Ubuntu 18.04 and Debian 9 usually require blacklisting bochs_drm so they will boot after install. This can be done in one of two ways

In /etc/modprobe.d/blacklist.conf, add

```
blacklist bochs_drm
```

or add to kernel command line

```
modprobe.blacklist=bochs_drm
```

- JIRA Issue: OXT-806

6.11. Disabling Wayland and resolving non-standard resolutions in Ubuntu 18.04

Ubuntu 18.04 guests require Wayland to be disabled. To disable it, uncomment

```
#WaylandEnable=False
```

in /etc/gdm3/custom.conf and/or /etc/gdm3/daemon.conf.

Sometimes, Ubuntu has issues with non-standard resolutions that manifests as just a black screen. Running the following commands in guest should resolve the issues.

```
sudo apt install --reinstall xserver-xorg-video-intel xserver-xorg-core
sudo apt install xserver-xorg
sudo dpkg-reconfigure xserver-xorg
sudo apt-get install xvfb xfonts-100dpi xfonts-75dpi xfstt

Edit /etc/default/grub
GRUB_GFXMODE=1280x960,1280x800,1280x720,1152x768,1152x700,1024x768,800x600
GRUB_PAYLOAD_LINUX=keep
sudo update-grub
sudo reboot
```

For reference: https://xenserver.org/blog/entry/increasing-ubuntu-s-resolution.html

- JIRA Issue: OXT-1661

6.12. Upgrades from 8.0.1 to 9.0.0 with host UEFI fail measurement after upgrade

Under 8.0.1, UEFI installs are Static Root of Trust for Measurement (SRTM) only. 9.0.0 uses both SRTM and DRTM. In order to predict the PCR values for DRTM PCRs 17, 18, and 19, the platform must have first booted with DRTM so insight can be gained from the values in those PCRs. Under SRTM-only boots, 17, 18, and 19 values are all 0xf's, making it impossible to forward seal such that measurement will succeed on the subsequent boot if upgrading from SRTM to SRTM+DRTM, in the case of 8.0.1 to 9.0.0.

Therefore, the administrator should expect to reseal the platform on first boot after this upgrade is complete.

- JIRA Issue: OXT-1659

6.13. Using an addon GPU as the Primary Display Device is unsupported

Always use the onboard display device as the primary display device in your system's BIOS. Using "auto" or an addon GPU as primary is unsupported, and will result in a crash. Additionally on some Dell machines, an addon GPU may override what the system considers to be the "integrated" GPU depending on the x16 PCI slot its inserted into.

- JIRA Issue: OXT-1601 OXT-1603

6.14. PV Disk Drivers have been removed from Windows tools

Emulated AHCI provides higher performance than both emulated IDE and PV. Upgrading OpenXT with guests that have guest tools installed should reinstall the new guest tools from the upgraded build. Additionally, the existing guest should be switched to using emulated AHCI disk type.

```
xec-vm -n <guest vm name> set hdtype ahci
```

- JIRA Issue: OXT-1559

6.15. Docked laptops may produce inconsistent PCR measurements between docked and undocked configurations

Due to how vendor firmware extends measurements into some PCRs, docked and undocked configurations for a laptop may produce different measurements. This would be observed by, for example, a measurement failure at boot time when the laptop is off the dock, as opposed to successful boot when the laptop is on the dock. Please handle your usecase accordingly.

- JIRA Issue: OXT-1594

6.16. Custom NDVMs that do not use network-slave

For custom NDVMs and service VMs that do not include network-slave, db-rm /vm/$uuid/config/nic/$N/network for any guests using network-slave-less network backends.

When a NDVM or service vm is restarted, xenmgr will re-attched any Xen netfront drivers to the new network backends. To confirm attachment, xenmgr will RPC through network-daemon to network-slave for any NICs with a defined "network" (/vm/$uuid/config/nic/$N/network). If the NDVM/service VM does not run network-slave, db-rm the "network" key to avoid triggering RPC calls which will go unanswered.

- JIRA Issue: OXT-1595

6.17. Disable Hyperthreading on Intel devices

For security purposes, hyperthreading should be disabled in xen running on Intel devices. OpenXT 9.0.0 disables Hyperthreading By default, by including the following option to the Xen command line:

```
smt=0
```

It is extremely recommended not to remove this value.

- JIRA Issue: OXT-1433

7. Contributors

- Jason Andryuk <jandryuk@gmail.com>
- Jed <lejosnej@ainfosec.com>
- Chris <rogersc@ainfosec.com>
- Mahantesh Salimath <salimathm@ainfosec.com>
- Jafar Al-Gharaibeh <jafar@atcorp.com>
- Christopher Clark <christopher.clark6@baesystems.com>
- Chris Rogers <rogersc@ainfosec.com>
- Kevin Pearson <kevin.pearson@ortmanconsulting.com>
- Nicholas Tsirakis <tsirakisn@ainfosec.com>
- Mahantesh Salimath <mahantesh.openxt@gmail.com>
- Daniel P. Smith <dpsmith@apertussolutions.com>
- turnerr <turnerr@ainfosec.com>
- Tyler McGavran <mcgavrant@ainfosec.com>
- Richard Turner <turnerr@ainfosec.com>
- Tim Konick <konickt@ainfosec.com>
- Eric Chanudet <chanudete@ainfosec.com>
- Tamas K Lengyel <lengyelt@ainfosec.com>

Appendix A: License