QEMU for Xen secure by default
Deprivileging the PC system emulator

Ian Jackson <ian.jackson@eu.citrix.com>
FOSDEM 2016
with assistance from Stefano Stabellini
guest

Xen PV driver

Xen PV protocol

Xen PV backend
(usually)
dom0
kernel
Device driver

PV

guest

IDE driver

mmio, dma, etc.

qemu

Emulated IDE controller

(usually), syscalls

(usu.dom0)
kernels
Device driver

HVM
<table>
<thead>
<tr>
<th>Advisory</th>
<th>Public release</th>
<th>CVE(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>XSA-164</td>
<td>2015-12-17 12:00</td>
<td>CVE-2015-8554</td>
<td>qemu-dm buffer overrun in MSI-X handling</td>
</tr>
<tr>
<td>XSA-162</td>
<td>2015-11-30 06:00</td>
<td>CVE-2015-7504</td>
<td>heap buffer overflow vulnerability in pcnet emulator</td>
</tr>
<tr>
<td>XSA-140</td>
<td>2015-08-03 12:00</td>
<td>CVE-2015-5165</td>
<td>QEMU leak of uninitialized heap memory in rtl8139 device model</td>
</tr>
<tr>
<td>XSA-139</td>
<td>2015-08-03 12:00</td>
<td>CVE-2015-5166</td>
<td>Use after free in QEMU/Xen block unplug protocol</td>
</tr>
<tr>
<td>XSA-138</td>
<td>2015-07-27 12:00</td>
<td>CVE-2015-5154</td>
<td>QEMU heap overflow flaw while processing certain ATAPI commands.</td>
</tr>
<tr>
<td>XSA-135</td>
<td>2015-06-10 13:10</td>
<td>CVE-2015-3209</td>
<td>Heap overflow in QEMU PCNET controller, allowing guest-&gt;host escape</td>
</tr>
<tr>
<td>XSA-131</td>
<td>2015-06-02 12:00</td>
<td>CVE-2015-4106</td>
<td>Unmediated PCI register access in qemu</td>
</tr>
<tr>
<td>XSA-130</td>
<td>2015-06-02 12:00</td>
<td>CVE-2015-4105</td>
<td>Guest triggerable qemu MSI-X pass-through error messages</td>
</tr>
</tbody>
</table>

from Xen Security Team advisories page, http://xenbits.xen.org/xsa/
Xen on x86 modes, and device model bug implications

Current status for users of upstream Xen and distros

<table>
<thead>
<tr>
<th>Mode</th>
<th>Status</th>
<th>Device model bugs mean</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV</td>
<td>Fully supported</td>
<td>Safe (no DM)</td>
<td>Only modified guests</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu in dom0</td>
<td>Fully supported</td>
<td>Vulnerable</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu stub DM</td>
<td>Upstream but not in most distros.</td>
<td>Safe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ancient qemu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Build system problems</td>
</tr>
</tbody>
</table>
## Xen on x86 modes, and device model bug implications

**Current status for users of upstream Xen and distros**

**and future plans**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Device Model</th>
<th>Status</th>
<th>Device Model Bugs Mean</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV</td>
<td></td>
<td>Fully supported</td>
<td>Safe (no DM)</td>
<td>Only modified guests</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu in dom0 as root</td>
<td>Fully supported</td>
<td>Vulnerable</td>
<td>Current default</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu stub DM qemu-xen-trad.</td>
<td>Upstream but not in most distros.</td>
<td>Safe</td>
<td>Ancient qemu Build system problems</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu stub DM rump kernel</td>
<td>In progress</td>
<td>Safe</td>
<td>Rump build system is mini distro</td>
</tr>
<tr>
<td>HVM</td>
<td>qemu dom0 not as root</td>
<td><strong>Targeting Xen 4.7</strong></td>
<td>No privilege esc. Maybe dom0 DoS</td>
<td>Defence in depth Hopefully, will be default</td>
</tr>
</tbody>
</table>
**Dom0 Kernel**
- Net, storage etc. access

**Guest**
- Domain control
- "Dma" mmio handling
- Ioport handling
- Interrupts
- Etc. access

**Underlying Disk, Network, Etc.**

**Qemu Device Model Process**

**Xen**
# Xen on x86 modes, and device model bug implications

Current status for users of upstream Xen and distros and future plans

<table>
<thead>
<tr>
<th></th>
<th>Status</th>
<th>Device model bugs mean</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PV</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fully supported</td>
<td>Safe (no DM)</td>
<td>Only modified guests</td>
</tr>
<tr>
<td><strong>HVM</strong></td>
<td>qemu in dom0 as root</td>
<td>Fully supported</td>
<td>Vulnerable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Current default</td>
</tr>
<tr>
<td><strong>HVM</strong></td>
<td>qemu stub DM</td>
<td>Upstream but not in most distros.</td>
<td>Safe</td>
</tr>
<tr>
<td></td>
<td>qemu-xen-trad.</td>
<td></td>
<td>Ancient qemu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Build system problems</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HVM</strong></td>
<td>qemu stub DM</td>
<td>In progress</td>
<td>Safe</td>
</tr>
<tr>
<td></td>
<td>rump kernel</td>
<td></td>
<td>Rump build system is mini distro</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hard work!</td>
<td></td>
</tr>
<tr>
<td><strong>HVM</strong></td>
<td>qemu dom0 not as root</td>
<td><strong>Targeting Xen 4.7</strong></td>
<td>No privilege esc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Defence in depth</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hopefully, will be default</td>
</tr>
</tbody>
</table>