Written by Marco Attard
15 May 2015

CrowdStrike discovers a security vulnerability that is possibly even greater than last year's Heartbleed-- Venom, a bug providing hackers with access to datacentre hypervisors and network-connected devices.

An acronym for "Virtualised Environment Neglected Operations Manipulation", Venom (aka CVE-2015-3456) affects one of the most widely ignored pieces of virtualisation platform components, the virtual floppy drive. It has been part of the open-source computer emulator QEMU since 2004, and is found in many modern hypervisors, including XEN, KVM and VirtualBox.

VMware, Microsoft Hyper-V and Bochs hypervisors are not affected.

As CrowdStrike puts it, hackers can crash an entire hypervisor by sending special code to the flawed floppy disk controller. This allows the hacker to break out of their own virtual machine (VM) and access other VMs, including those owned by other people or companies.

It is arguably more dangerous than the Heartbleed, since it "applies to a wide array of virtualisation platforms, works on default configurations, and allows for direct arbitrary code execution."

In good news, CrowdStrike says no code exploiting the bug is publicly known, at least so far. The security researcher has already notified the developers of the affected systems, who should be releasing maintenance updates soon.

Go Venom