'Venom' vulnerability found in virtualization platforms allows complete access to all user data

May 14 2015, by Bob Yirka

Credit: Wikipedia

Security firm CrowdStrike has found a potentially serious vulnerability in a type of virtualization platform that could allow a hacker to breakout from its own virtual space and into the space of other users on a shared server. That means that millions of uses relying on the security of data stored "in the cloud" could be put at risk.

The vulnerability has been labeled Virtualized Environment Neglected Operations Manipulation (VENOM) because of the way it works (and likely its menacing sound). It takes advantage of a previously unknown problem with a virtual floppy disk controller used by the underlying operating system—if sent a particular string of characters by a hacker, officials with CrowdStrike report, it can be made to crash allowing entry to the hypervisor—a part of the operating system that interfaces with the individual supervisors that run the virtual environments for cloud customers. And that means that such a hacker would gain access to every piece of data on the server, potentially putting millions of people's data at risk of exposure. Virtual floppy disks are not often used by such systems but remain in place as legacy devices to maintain compatibility with older systems.

Fortunately, the problem is so arcane, that hackers apparently have not noticed it either—because of that, while it is potentially much more serious of a threat than the Heartbleed bug found last year, it does not appear to be as damaging. The vulnerability has existed since 2004, and yet there are no known instances of anyone actually using it to gain access to cloud data. But now that it has been found and publicized, hackers will know about it, which is why a patch to fix the problem has been issued by Oracle and others. The vulnerability impacts platforms based on the open source computer emulator QEMU, such as VirtualBox, KVN and Xen (which can include machines running Mac OS X, Windows, Linux and others) but not VMware, Bochs hypervisors or Microsoft Hyper-V.

CrowdStrike suggests that cloud customers worried about the security of their data contact their host to find out if their data is on the type of server impacted, and if so, ask what is being done close the vulnerability.

More information: cve.mitre.org/cgi-bin/cvename. … i?name=CVE-2015-3456