National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Targeted Security Alert

VENOM VULNERABILITY

Original Issue Date: May 15, 2015

Severity Rating: High

Affected Systems:

- Operating Systems – Windows, Linux, Mac OS, etc.
- Virtual machines - QEMU, Xen, KVM, VirtualBox and other derivatives of these products

Description:

A critical virtual machine escape vulnerability dubbed as VENOM (Virtualised Environment Neglected Operations Manipulation) has been discovered by security researchers. The vulnerability existed since 2004, when the virtual Floppy Disk Controller was first added to the QEMU codebase but has now been detected.

The vulnerability resides in the virtual floppy drive code part - QEMU's virtual Floppy Disk Controller (FDC) used by many computer virtualization platforms. Since the VENOM vulnerability exists in the hypervisor's codebase, the vulnerability is agnostic of the host operating system. VMware, Microsoft Hyper-V, and Bochs hypervisors are not impacted by this vulnerability.

This vulnerability can allow an attacker to escape from the confines of an affected virtual machine (VM) guest and gain code-execution access to the host. Successful exploitation of the vulnerability could open access to the host system and other VMs running on that host, significant elevated access to the host's local network and adjacent systems. Though the VENOM vulnerability can also impact the guest operating system, exploitation of VENOM would require administrative or root privileges in the guest operating system.

Methodology:

The guest operating system communicates with the FDC by sending commands such as seek, read, write, format, etc. to the FDC's input/output port. QEMU's virtual FDC uses a fixed-size buffer for storing these commands and their associated data parameters. The FDC keeps track of how much data to expect for each command and, after all expected data for a given command is received from the guest system, the FDC executes the command and clears the buffer for the next command.

This buffer reset is performed immediately at the completion of processing for all FDC commands, except for two of the defined commands. This can allow an attacker to send these commands and specially crafted parameter data from the guest system to the FDC to overflow the data buffer and execute arbitrary code in the context of the host's hypervisor process.

Impact:

Successful exploitation of the VENOM vulnerability can expose access to corporate intellectual property, sensitive and personally identifiable information which can impact organisations and end users that rely on affected VMs for the allocation of shared computing resources, connectivity, storage, security and privacy.

CVE Information:

CVE-2015-3456

Testing the VENOM Vulnerability

VENOM can be tested through the following vulnerability detector:

- Red Hat (QEMU Vulnerability detector): https://idp.redhat.com/idp/

Workarounds:

1. Administrators of systems notably Xen, KVM, or the native QEMU client are advised to review and apply the latest patches to address this vulnerability.

2. If you have a vendor service or device using one of the affected hypervisors, contact the vendor's support team to see if their staff has applied the latest VENOM patches.

Available Vendors' Patches:

The following vendors have already released patches to address the VENOM vulnerability:

- QEMU: http://git.qemu.org/?p=qemu.git;a=commitdiff;h=e907746266721f305d67bc0718795fedee2e824c
- Xen Project: http://xenbits.xen.org/xsa/advisory-133.html
- Red Hat: https://access.redhat.com/articles/1444903
- Citrix: http://support.citrix.com/article/CTX201078
- FireEye: https://www.fireeye.com/content/dam/fireeye-www/support/pdfs/fireeye-venom-vulnerability.pdf
- Linode: https://blog.linode.com/2015/05/13/venom-cve-2015-3456-vulnerability-and-linode/
- Rackspace: https://community.rackspace.com/general/f/53/t/5187
- Ubuntu: http://www.ubuntu.com/usn/usn-2608-1/
- Debian: https://security-tracker.debian.org/tracker/CVE-2015-3456
- Suse: https://www.suse.com/support/kb/doc.php?id=7016497
- DigitalOcean: https://www.digitalocean.com/company/blog/update-on-CVE-2015-3456/
- f5: https://support.f5.com/kb/en-us/solutions/public/16000/600/sol16620.html

- Joyent: https://help.joyent.com/entries/68099220-Security-Advisory-on-Venom-CVE-2015-3456-in-KVM-QEMU
- Liquid Web: http://www.liquidweb.com/kb/information-on-cve-2015-3456-qemu-vulnerability-venom/
- UpCloud: http://status.upcloud.com/incidents/tt05z2340wws

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu