New Vuln in Xen – Hypervisors Require Hypervigilance

Bill Weinberg | Senior Director and Analyst, Open Source Strategy | The Linux Foundation | Nov 4, 2015

Developers of the Xen Hypervisor recently revealed that a new critical vulnerability had surfaced in this key piece of system software. The first, Venom (CVE-2015-3456) became known in May 2015. Another, CVE-2015-5154 cropped up in July. And now, a new high profile vulnerability, CVE-2015-7835, has joined the other two.

The Xen project delivers a hypervisor (a.k.a. a virtual machine manager), code that enables servers in the data center and the cloud to act like much larger collections of isolated virtual servers. In this role, Xen powers large swathes of cloud infrastructure. In particular, Amazon Web Services builds upon its capabilities. Xen also has applications on the desktop (as an application-level Type II hypervisor). Key parts of Xen (QEMU) also find use in development environments and even embedded settings.

The three reported vulnerabilities enable malicious actors and/or guest software running on one virtual machine (VM) to "break through" the programmatic isolation among multiple VMs. Exploiting this vulnerability would let black hats take over other guest systems on the same server, infiltrating network streams, exfiltrating data, and wreaking other types of cyber-havoc.

Inter-VM isolation, while enforced with hardware-based memory management, can be difficult to program and configure, leaving room for exploitable bugs. Vulnerabilities of this type (and most others) are almost never discovered by code analysis tools – of the 4,300+ vulns uncovered in open source code in 2014, 99% were ferreted out by researchers, not software quality tools. So subtle was CVE-2015-7835, that the faulty code lay undiagnosed for over 7 years.

So what can developers and integrators of Xen and other critical open source technologies do to protect themselves?

Initially, there's not a lot end-users and developers outside the Xen project really can do. The vulnerabilities in question were disclosed under embargo while a patch was developed. Luckily, there were no known exploits "in the wild", but zero-day exploits like these can command huge sums in the underground hacker economy.

Once a CVE is assigned, most organizations are still ill-prepared to discover they even have a problem, let alone devise remediation for it. That's where Black Duck can help. If your software portfolio includes affected versions of Xen (in this case, version 3.4 onwards), the Black Duck Hub and the Black Duck Suite will discover this component in your builds and immediately notify your dev team. As patches and new versions become available, Black Duck tools will keep your developers informed and recommend appropriate updates. Moreover, our industry leading Open Source Hygiene capabilities not only help protect your

apps and infrastructure from Xen-based vulnerabilities, but from critical security faults in thousands of the most popular and important open source projects.

But start monitoring your open source software soon – with a predicted 6000-8000 vulnerabilities likely to surface in open source code in 2015, that's over new 20 vulnerabilities reported EVERY DAY.