www.infosecwriters.com

Open Stack & Open Source Software Vulnerabilities

Maxton Richardson

4/16/2017

WWW.INFOSECWRITERS.COM

Open Stack is an open source software technology that's changing and developing the way we do business, but many are unaware of Open Stack technology. According to Business Wire, "The World Runs on Open Stack". Open Stack is "Backed by some of the biggest companies in software development". There are "Thousands of individual community members who support the growth, maintenance, & development of Open Stack. Many big industries utilize Open Stack such as the Auto-Industry, media, finance, commerce, telecom, and energy. People all over the world use Open Stack daily, but very seldom people are aware of Open Stack technology. As stated by Opensource.com, "many think that Open Stack is the future of cloud computing."

"Open Stack is a set of software tools for managing cloud computing platforms for public & private clouds." (opensource.com) Open Stack is managed by the Open Stack Foundation, which is a non-profit organization that oversees the development and community-building around the project. OpenStack allows users to deploy virtual machines and other instances that handle different tasks for managing a cloud environment on the fly. Open Stack makes horizontal scaling easy. What do I mean by that? Horizontal scaling is when two or more tasks run concurrently. In Open Stack, tasks that benefit from running concurrently can easily serve multiple users on the fly by spinning up more instances, all of which are communicating with one another, but scaling quickly & easily as the application gains more users.

As we know, the cloud provides computing for end users in a remote environment. Typically, the industry refers to cloud computing as a service (such as software as a service, platform as a service, or infrastructure as a service). Open Stack falls under the category of Infrastructure as a service category. Open Stack provides infrastructure which makes it easy for

WWW.INFOSECWRITERS.COM

users to quickly add new instances. Typically, Open Stack runs a platform upon which a developer can create software applications that are delivered to end users.

Open Source Software may be a familiar technology that most people in the IT profession are familiar with. Open Source software basically means that the source code is open to the public. Anyone who chooses to make changes to the source code can do so as they please. Once modifications & changes are made, these changes can be freely shared back out to the community. Open Stack is Open Source Software.

Due to the Open Source nature of Open Stack, anyone can add additional components to OpenStack to meet the needs of developers. Open Stack is made up of a variety of moving parts. The Open Stack community has identified 9 key components that are considered to be the "core" of Open Stack. These "core" components are distributed as part of any Open Stack system & are officially maintained by the Open Stack community. The 9 "core" components of Open Stack are Nova, Swift, Cinder, Neutron, Horizon, Keystone, Glance, Ceilometer, and Heat.

Nova is the primary computing engine behind Open Stack. Nova is utilized by deploying and managing large numbers of virtual machines, as well as other instances to handle computing tasks. Swift is a storage for objects and files used for Open Stack. Typically, traditional storage processes refer to files by their location on a disk drive; however, with Swift developers can refer to a unique identifier referring to the file or piece of information, and allow Open Stack to decide where to store the information. Swift grants developers the luxury of storage scaling. Developers do not have to worry about running out of storage capacity on a single system behind the software. Swift also relieves the developer of deciding how the data will be backed up. Swift allows the system to make the decision on where to store the data & how it's backed up in case of machine (or network) failure. Cinder is another storage component of Open Stack.

WWW.INFOSECWRITERS.COM

Cinder is a block storage component which refers back to the more commonly known & traditional idea of the computer accessing specific locations on a disk drive. Cinder prioritizes speed, therefore in scenarios where speed is the most important factor, Cinder would be preferred over Swift. Neutron is considered to be "the glue that holds Open Stack together" (opensource.com). The Neutron component of Open Stack provides networking capability for Open Stack, which ensures that each component of Open Stack can communicate quickly and efficiently. Horizon is the sole graphical interface for Open Stack which provides tools for system administrators to view & manage the cloud as needed. Keystone protects the integrity of data in OpenStack by providing identity services for users so they can access their services & unauthorized users cannot. Keystone is essentially a central list of all users of the Open Stack cloud, mapped against all of services provided by the cloud. Glance provides image (referring to virtual copies of hard disks) services for Open Stack. Glance utilizes these images as templates when deploying new virtual machine instances. Ceilometer keeps track of system usage of individual users on the cloud, and also allows the cloud to provide billing services based on individual's system usage on the cloud. It also keeps a count of user's system usage of various components of an Open Stack cloud. Heat is known as "the orchestration component that helps manage the infrastructure as needed" (opensource.com). Heat allows developers to store requirements of a cloud application in a file which defines what resources are necessary for that application.

One of the most important facts about Open Stack that needs to be taken into consideration is that Open Stack is Open Source software. Open Stack has the benefit of thousands of developers all over the world working together to develop the strongest, and most secure product possible. Studies show that defects are located and resolved faster in Open

WWW.INFOSECWRITERS.COM

Source Software (OSS) compared to Closed Source Software (CSS). The more developers that have access to make corrections to the software, the more likely problems will be found at a quicker pace. Open Source software is known for being highly reliable, and helping organizations & businesses become more flexible. On the other hand, because source code to OSS is made available to developers all over the world for improvement, it also enables users with malicious intent to exploit vulnerabilities causing harm to the network.

OSS itself isn't more superior than CSS. In certain cases, CSS may be preferred over OSS. Some factors need to be taken into consideration when deciding to incorporate OSS vs. CSS into a business, such as cost advantage or source code. OSS claims to be free of charge; however, other costs need to be considered such as cost of licensing. Source code in OSS may offer availability that leads to higher quality in service, but the developers who have access to the code may not have the knowledge necessary to apply modifications necessary.

There are thousands of Open Source security vulnerabilities reported every year. Fortunately, often developers can find vulnerabilities before malicious attackers can, allowing developers to make changes in the software before any real damage is done. Of the Open Source security vulnerabilities that were reported in 2016, here are the top 7 most talked about security vulnerabilities: GLIBC Vulnerability, Quadrooter, Drown Attack, Zero-Day Kernel Vulnerability, Critical MySQL Database Vulnerability, Linux Kernel Vulnerability, and the Open JDK Vulnerability (The Top Open Source Security Vulnerabilities of 2016).

The Glibc vulnerability affected most Linux servers and framework such as Python, PHP, Rails, as well as API web servers which utilize the GNC Library. The Glibc vulnerability enabled hackers to compromise apps with a man-in-the-middle attack. Exploiting the Glibc vulnerability with the man-in-the-middle attack allowed the possibility of unauthorized personnel

WWW.INFOSECWRITERS.COM

to take control of a user's system. One of the sole reasons this vulnerability was such a big issue, is because it was first introduced to Glibc 2.9, which was released in 2008. Meaning the Glibc vulnerability was around for 8 years before developers discovered its existence. Another reason the Glibc vulnerability was such a big issue is because Glibc is one of the oldest Open Source libraries released. RedHat engineer Florian Weimer explains the attack: "An attack would first force a system to make a specific DNS queries, using domain names controlled by the attacker. The attacker would then have to run custom-written DNS server software, which generates crafted responses that trigger the vulnerability." (Mimoso) It's believed that the most direct exploitation vector would be a man-in-the-middle attack. Researcher, cofounder and chief scientist at White Ops, Dan Kaminsky says, "While man-in-the-middle attacks are problematic, it would be much worse if the flaw were exploitable through DNS caching-only servers." (Mimoso) Luckily, developers were able to notice this vulnerability before attackers were able to exploit it. (which is hard to believe considering it was exploitable for 8 years). The Glibc vulnerability was discovered by researchers at Red Hat and Google. The researchers were able to privately disclose the issue to upstream Glibc maintainers. After upgrades were made to the software, patches were made available to Linux distributions that used Glibc. Updates made for Linux distributions include security fixes, as well as bug fixes & performance enhancements. Temporary mitigation methods were advised until patches were made available. One of the mitigation techniques included limiting the size of UDP or TCP responses that were accepted by a DNS revolver, and ensure that DNS queries are sent only to servers that limit the response size.

WWW.INFOSECWRITERS.COM

There is software that is created to mitigate the Glibc vulnerability. One software, known as BlackDuck Hub, is a software application created to prevent to Glibc vulnerability. The BlackDuck Hub application essentially scans for the Glibc vulnerability.

For Open Stack, similar vulnerabilities that are found in popular Open Source software can arise. In my research, I was unable to find any security vulnerabilities directly pertaining to Open Stack, which leads me to believe that Open Stack one of the more secure OSS products on the market. To reinforce that assumption, Open Stack received the "Core Infrastructure Initiative (CII) Best Practices Badge" from the Linux Foundation. CTO of the Linux Foundation, Nicko van Someren says, "Open Stack is rapidly becoming the cornerstone of public and private cloud deployments across the internet." (openstack.org)

WWW.INFOSECWRITERS.COM

References

Open Source Cloud Computing Software. (n.d.). Retrieved April 16, 2017, from https://www.openstack.org/news/view/243/openstack-earns-core-infrastructure-initiative-best-practices-badge-for-security,-quality-and-stability

What is OpenStack? (n.d.). Retrieved April 16, 2017, from https://opensource.com/resources/what-is-openstack

C. (2015, June 26). 7 Main Advantages and Disadvantages of Open Source Software. Retrieved April 16, 2017, from http://connectusfund.org/7-main-advantages-and-disadvantages-of-open-source-software

Security. (n.d.). Retrieved April 16, 2017, from https://wiki.openstack.org/wiki/Security

WWW.INFOSECWRITERS.COM

The Top Open Source Security Vulnerabilities of 2016. (2017, April 04). Retrieved April 16, 2017, from https://www.whitesourcesoftware.com/whitesource-blog/open-source-security-vulnerability/

Mimoso, M. (2016, February 17). Magnitude of glibc Vulnerability Coming to Light. Retrieved April 16, 2017, from https://threatpost.com/magnitude-of-glibc-vulnerability-coming-to-light/116296/

Mimoso, M. (2016, February 17). Critical glibc Vulnerability Puts All Linux Machines at Risk. Retrieved April 16, 2017, from https://threatpost.com/critical-glibc-vulnerability-puts-all-linux-machines-at-risk/116261/

OpenStack Gains Ground in the Enterprise With Business-Critical Workloads ... (2016, October 25). Retrieved April 16, 2017, from https://youtu.be/IK_QMZr4A5c

Finding the GLIBC Vulnerability - CVE-2015-7547. (2016, February 19). Retrieved April 16, 2017, from https://youtu.be/hkryI6eapOA

OpenStack Gains Ground in the Enterprise With Business-Critical Workloads Running on Larger Deployments Across Diverse Industries: 451 Research. (2016, October 25). Retrieved April 16, 2017, from http://www.businesswire.com/news/home/20161025005506/en/OpenStack-Gains-Ground-Enterprise-Business-Critical-Workloads-Running

* Laplante, P., Gold, A., & Costello, T. (2007). Open source software: Is it worth converting? IT Professional Magazine, 9(4), 28-33. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.1109/MITP.2007.72

*Ven, Kris., Verelst, Jan., Mannaert, Herwig. (2008). Should You Adopt Open Source Software? IEEE Software, 25(3), 54-59. Retrieved April 16, 2017, from http://ieeexplore.ieee.org/document/4497765/

WWW.INFOSECWRITERS.COM