How Much Your Cloud Management Platform Is Secure? OpenStack Use Case

Najat Tissir[1(✉)], Said ElKafhali[2], and Noureddine Aboutabit[1]

[1] Process Engineering, Computer Science and Mathematics Laboratory, National School of Applied Sciences of Khouribga, Sultan Moulay Slimane University, Beni Mellal, Morocco
tissir.najat@gmail.com, n.aboutabit@usms.ma

[2] Faculty of Sciences and Techniques, Computer, Networks, Mobility and Modeling Laboratory: IR2M, Hassan First University of Settat, 26000 Settat, Morocco
said.elkafhali@uhp.ac.ma

Abstract. Cloud computing still one of the most hyped IT innovations. It envisages a world where components can be rapidly released, implemented, and scaled up and down providing an on-demand utility-like model of allocation and consumption. Moreover, Cloud Management Platform CMP is considered one of its typical components. It is a software product that deploys and manages a Cloud infrastructure. OpenStack, as the most widely adopted platform, has got more and more attention. It aims to be competitive compared to other platforms, like Amazon Web Services (AWS). Furthermore, the adoption of cloud solutions introduces security and privacy concerns. OpenStack is no exception, and security concerns are present in its lifecycle which makes its security analysis a crucial mission. Therefore, this paper firstly presents a state of the art of OpenStack components, sub-components, and their interaction. Then, it focuses principally on an analysis of the most common vulnerabilities affected by OpenStack. The analysis is based on ten years of security reports. Our work leads to have a good comprehension of the OpenStack project, identify its vulnerability trends, and characterize comprehensively its security issues.

Keywords: Cloud computing · OpenStack · Security · Vulnerabilities

1 Introduction

With the rising popularity of cloud computing in recent years, organizations dealing with traditional computing environments could benefit from the cloud without doing any upfront investment. Moreover, the cloud provides agility and speed with economies of scale benefits. However, organizations will still have some applications that run locally. In fact, according to [1] by 2021, 94% of workloads and compute instances will be processed by cloud data centers, while 6% will be processed by traditional data centers (see Fig. 1). Also, the Global Public Cloud Market size is expected to reach $488.5 billion by 2026, rising at a market growth of 16% CAGR during the forecast period [2].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021
M. Ben Ahmed et al. (Eds.): SCA 2020, LNNS 183, pp. 1117–1129, 2021.
https://doi.org/10.1007/978-3-030-66840-2_85

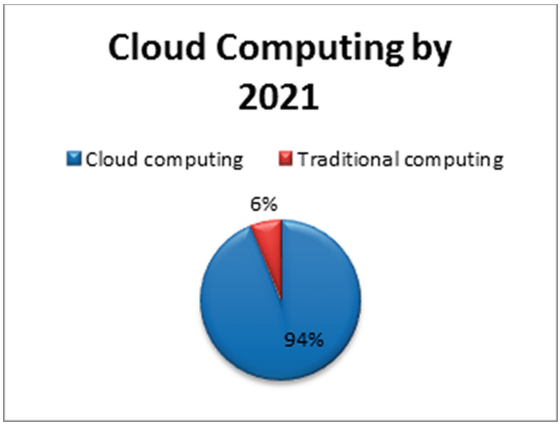

Fig. 1. Increase the use of Cloud Computing by 2021

Furthermore, Cloud Computing can be helpful in calamitous moments, such as Covid-19 Coronavirus. In fact, according to [3], Cloud Computing besides AI solutions were developed by Alibaba to help China predict the peak, size, and duration of the outbreak. Besides, authors in [4] argued that Cloud services can be used to enhance the prediction process using high-speed computations. Additionally, Javaid *et al.* [5] confirmed that the Salesforce Care solution for healthcare providers received a large number of requests due to COVID-19. Therefore, Cloud Computing, being public or private; for individuals or organizations; in healthcare domain or another, keeps increasing and guiding the future toward a digital world.

Actually, organizations can use cloud applications commonly called Software as a Service (SaaS) [6], which really means applications running at data centers owned by a cloud operator and accessed via the internet. Organizations can also use cloud development platforms which are commonly called Platform as a Service (PaaS) for their software developers. At last, organizations can leverage the cloud by running some of their applications on computing resources in data centers across the Internet; this is commonly called the infrastructure as a Service (IaaS) consumption model [7]. Moreover, Fig. 2 presents the percentages of use of the three cloud service models compared to the total cloud workloads and compute instances from 2016 to 2021. IaaS is showing a decrease of 5%, while PaaS and SaaS are growing respectively by 1% and 4%. Besides, the SaaS model remains the first adapted model compared to other service models [1].

Cloud computing provides individual users and organizations with various capabilities, to store and process their data in third-party data centers. They may be located anywhere far from the user ranging in the distance from across the city to across the world. There are four major deployment models of the current clouds: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud.

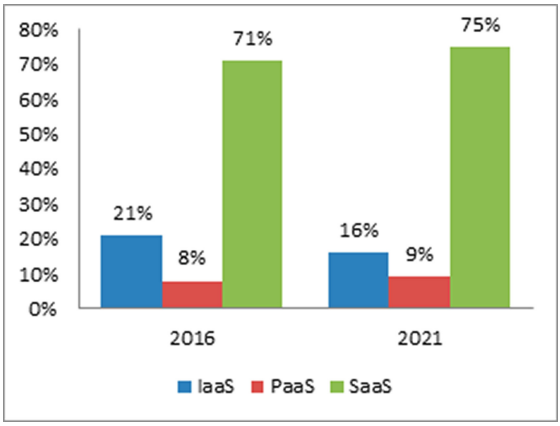

Fig. 2. Most popular cloud service model through 2021

Furthermore, individuals and companies have two options to enjoy Cloud Computing. They either opt for public cloud solutions, such as Amazon Web Services [8], and Microsoft Azure [9], or make their own private cloud infrastructure, and OpenStack [10] is the most popular non-proprietary software package of its kind. In this work, we concentrate on IaaS cloud systems. In addition to virtualization, IaaS systems principally consist of Cloud Management Platforms CMPs. A CMP, such as OpenStack, Eucalyptus [11], CloudStack [12], and OpenNebula [13], is a platform that deploys and manages a Cloud infrastructure.

Actually, OpenStack has emerged as an efficient infrastructure as a service platform, developed in 2010 as a joint project of Rackspace Hosting and NASA. It manages compute storage and networking resources throughout a data center. All resources may be controlled through a dashboard that gives administrators control while empowering their users to provision resources through a web interface. OpenStack can be used to implement both private and public clouds. Until now, OpenStack has released **22** versions from **A (Austin)** to **V (Victoria)**. During this evolution, functions of the system have been continuously improved [2]. The project aims to deliver solutions for all types of clouds by being simple to implement, massively scalable, and feature-rich. OpenStack turns many sets of hypervisors, storage, and network devices within a data center or across multiple data centers into pools of resources. Furthermore, OpenStack provides a cloud infrastructure with huge benefits in terms of resilience, performance and compatibility. In fact, OpenStack's performance was considered in [14] as the best among the cloud management platforms (Eucalyptus, Apache CloudStack). Also, authors in [15] argued that OpenStack presents the best percentage of resiliency, has more compatibility options, and is more stable compared to Apache CloudStack and OpenNebula cloud solutions.

The adoption of cloud solutions introduces security and privacy concerns due to the relocation of the resources and data to third-party infrastructures.

OpenStack is no exception, and security issues are present in its lifecycle [16]. During this paper we attempt to answer the following questions:

- *What characterizes more OpenStack in comparison to other cloud solutions?*
- *What are the different core and optional services of the OpenStack project?*
- *What are the most important OpenStack security issues?*
- *What type of vulnerabilities still affecting the OpenStack platform?*

Keeping all these questions in mind this paper has been designed to cover the different aspects of OpenStack's modular architecture, analyze 9 years of OpenStack security reports, discuss a set of vulnerabilities affecting the framework, and lastly try to detail the most important characteristics of current OpenStack vulnerabilities.

The remainder of this paper is divided into five sections: Sect. 2 describes the main modules of OpenStack architecture. Section 3 presents the related work. Section 4 provides an analysis of current vulnerabilities of OpenStack. Finally, the Sect. 5 states the conclusion.

2 OpenStack Architecture

OpenStack has a modular architecture with various code names for its component projects. It is a powerful and highly configurable integration engine with a set of core projects. What makes OpenStack quite special is that is a collection of multiple software and not a big piece of monolithic software. Actually, it consists of several independent parts called OpenStack services. Each service is designed to work together to provide a complete infrastructure as a service. And the integration between services is facilitated through public Application Programming Interfaces API that each service offers and in turn can consume. We have three ways to use OpenStack: via the horizon dashboard which may be the simplest, flexible, and easy way, via the command-line interface or the API. In general, all those three methods use API at the back end. Figure 3 describes the relationship between the most commonly deployed services across the OpenStack cloud.

2.1 Horizon (Dashboard)

Horizon [17] is the framework that provides the web interface for an easy management of instances and other OpenStack configuration. It is an ideal platform for end-users doing self-service, while the dashboard is the web interface built on top of that platform. Horizon gets the end-users' instructions and reaches the specific OpenStack service via its API and gives the instruction to that service with the help of the restore interface. The Horizon's design also allows for third party products and services such as billing, monitoring and additional management tools to be integrated. Service providers or any other user can customize the dashboard with their brands or they can change the look and feel of the gooey if they want to. Moreover, all the actions that are taken through the dashboard result in calls to the API to complete the task requested by the end-user.

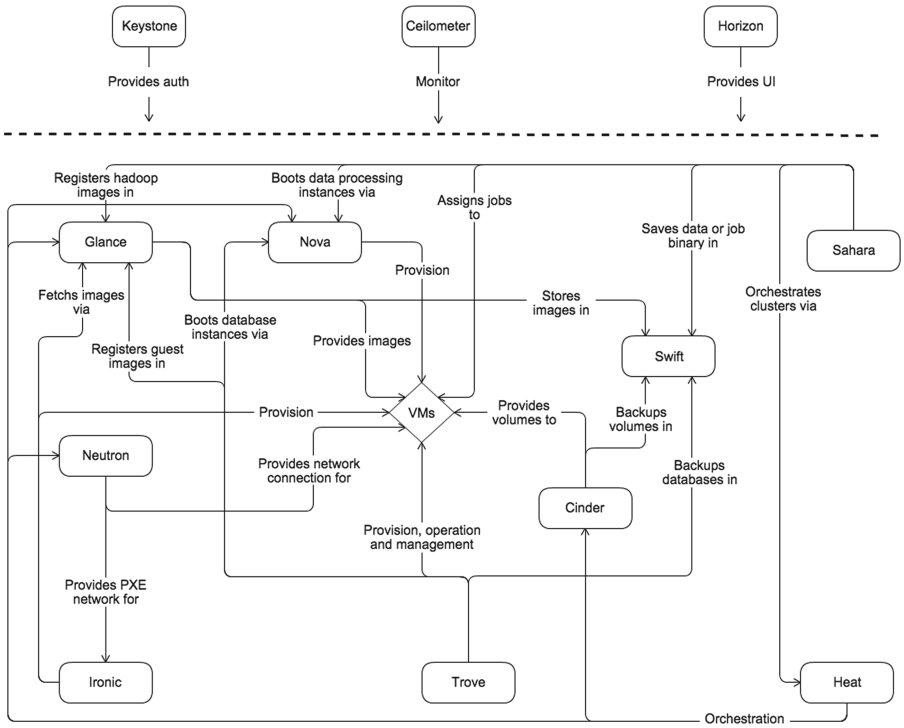

Fig. 3. OpenStack architecture [10]

2.2 Nova (Compute)

Nova [18,19] is one of the first two original and complicated projects of OpenStack. Nova is designed to manage and automate pools of computing resources and can work with available virtualization technologies, as well as, bare metal and high-performance computing configurations. It touches base with almost every component in OpenStack, such as networking, image services, and storage. Nova provides instance lifecycle management with its rich API. It is responsible for instance creation, scheduling, deletion, and size selection. Since VMs are created by the hypervisor, this makes Nova the hypervisor manager. It will manage these virtual machines on-demand across the hypervisor. Nova has an abstraction layer for computing drivers and this is what permits to choose which hypervisor to use. Furthermore, Nova talks to the hypervisor through an API or with an agent that needs to be installed on top of the hypervisor to manage it.

2.3 Neutron (Networking)

Neutron [20] is the project under the OpenStack tenant. It provides network connectivity as a service for instances running on a hypervisor. Neutron abstracts

ports, networks, and subnets and makes them programmable with the help of API. It also has a plugin architecture that makes it possible to integrate open source or proprietary vendor technologies and provide additional services that are similarly abstracted. Neutron has a modular architecture which could be deployed either in a centralized or distributed way depending on users' needs. Moreover, the service works by allowing users to create their virtual isolated networks and then attach interfaces to them. Those networks could remain isolated or could be connected to the rest of the world depending on requirements. Connectivity between internal networks is achieved by creating virtual routers to create routes between those virtual networks. Even a virtual router can be connected to a public network and a floating IP address that could be allocated to an instance to provide external access. One of the motivations for creating Neutron was to enable the ability, to create rich typologies including multi-tier networks with a lot of features, to enable options like using VXLAN and GRE tunnels, to have an extensible plugin architecture that does not limit OpenStack contributor's design and deployment choices, and to provide advanced services like load balancing, VPN, firewall and lots of other Layer 4 to all 7 services with the neutron.

2.4 Keystone (Identity)

Keystone [21] is an OpenStack identity service that provides central authentication for users and projects. The most important terms related to Keystone are User, Project, Role, Token, and Catalog. A user is a digital representation of a person, system, service, or something that gains access through Keystone. Users have a login and can access resources by using assigned tokens. The second term is a project or a tenant; it is a container that groups or isolates resources or identity objects. The third term is the role; it represents a set of rights and privileges attributed to users to perform a specific set of operations. The next one is a token; it is an alphanumeric text string that enables access to OpenStack APIs and resources. The identity Service issues a token to a user that includes a list of roles. When a user calls a service, that service interprets the user roles and determines which operations or resources each role grants access. Last not least a catalog; it is a sort of like the directory services for the OpenStack APIs. All of the components normally have different API endpoints by registering them with Keystone and letting Keystone keep a catalog of those endpoints. Moreover, to make an API call to one of these endpoints we just interact with Keystone during authentication and get the endpoint address from the catalog provided.

2.5 Glance (Image Service)

Glance [22] is a very stable and not so complex service of OpenStack and the services it provides are not complicated. It has a client-server architecture that provides a Rest API to the users through which requests to the server can be performed. Moreover, Glance is composed of multiple components coming together

to perform the required tasks to store and retrieve images and associated metadata per requested by a client.

2.6 Cinder (Block Storage)

Block storage is implemented in OpenStack by the Cinder project [23]. It mainly interacts with Nova providing persistent virtualized block devices for its instances. Volumes may be attached to a single instance at a time but maybe detached or re-attached to a different instance while retaining all data much like a USP drive. Cinder virtualizes the management of block storage devices and provides end-users with a self-service API to request and consume those resources without requiring any knowledge of where their storage is deployed. Cinder also manages snapshots and volume types.

2.7 Swift (Object Storage)

Swift [24] is an OpenStack store project. It works in a very simple way and that's what makes it so powerful and scalable, unlike Cinder that works at the block level. Also, it provides high concurrency by supporting lots of users. Swift is an eventually consistent system which means that all replicas are written at the same time, and failed replicas will be handled separately. Additionally, it permits to store by default 3 replicas and continually ensures the durability of the data by checksumming it and comparing it to the original checksum. The stored replicas are placed according to a hierarchy due to an as unique as possible algorithm. This algorithm first tries to put data in different regions then zones then servers and finally disks.

In addition to that, OpenStack contains other services providing access to infrastructure resources, like **ZUN**, it permits to treat containers as OpenStack-managed resource; **QINLING**, it permits to support server less functions; **IRONIC** is a Bare Metal Provisioning Service; **CYBORG** is Lifecycle management of accelerators; **MANILA**, it permits access to shared or distributed file systems; **OCTAVIA** is an open-source load balancer; **DESIGNATE**, it is a DNS service; **BARBICAN** is the key management service; **KARBOR**, it permits the protection of data and metadata; **SEARCHLIGHT** is an indexing and search service; **HEAT**, it is for orchestration; **SENLIN** is a clustering service; **MISTRAL** is a Workflow service; **ZAQAR** is a Messaging Service; **BLAZAR** is a resource reservation service; **AODH** is an alarming Service; **MAGNUM**; **SAHARA**; **TROVE** are for workload provision; **MASAKARI**; **MURANO**; **SOLUM**; **FREEZER** are for Application Lifecycle; and **EC2API** is a proxy [10].

3 Related Work

OpenStack, as a component of Infrastructure as a Service, is no different than any cloud computing platform in facing security challenges. It is the most widely

adopted cloud in the open-source world, but it could fail in the security side, especially Access Control, affirmed Yang Luo *et al.* [25]. Accordingly, the access control mechanisms in OpenStack are still inadequate to provide a strong security, and 105 out of 371 operations are performed without any access control. So, the authors propose a security framework called OpenStack Security Modules OSM that permits to let access control be a standalone part of the cloud, differentiate between the cloud administrators and tenant administrators, and finally, users can submit directly their policy to the cloud. Also, authors in [26] focused on private clouds and studied three attacks (Code injection XSS, Remote control CSRF, and UI-Redressing) caused by vulnerabilities in Cloud Control Interface CCI. But, in the case of OpenStack and XSS attack, the vulnerability was filed under CVE-2014-3594. While authors in [27] focused on two security issues in private cloud platforms: Data breaches and weak authentication, and identified related vulnerabilities with a demonstration based on CloudStack. Additionally, the paper [28] studied Keystone authentication vulnerability and proposed to combine both symmetric and asymmetric encryption authentication model. Furthermore, Madi *et al.* [29] proposed an automated framework that allows auditing the cloud infrastructure and integrate it into OpenStack. On the other hand, researchers in [30] analyzed the already identified vulnerabilities and threats in OpenStack, especially Nova component.

In addition to that, Anisetti *et al.* [31] focused, in their work, on evaluating the security assurance of OpenStack and defining its security benchmark. They proposed a 'Moon Cloud' platform composed of a set of recommendations for continuous cloud security verification. Additionally, authors in [32] opt for analysis security for OpenStack private cloud. They analyzed security of cloud nodes and hosted virtual machines using vulnerabilities scanners, and listed the opened ports and their limitations. Then, they applied the necessary firewall rules. Moreover, Hugan *et al.* [33] provided a holistic security analysis. The analysis is based on Universally Composable UC security framework. Authors introduced a novel tokening mechanism-RAFT- instead of Fernet Token; they aimed to enforce OpenStack security.

4 Openstack Security: Analysis of Vulnerabilities

Common Vulnerabilities and Exposures CVE [34] is a public on-line database that permits to provide a common reference to all OpenStack vulnerabilities. The National Vulnerability Database NVD [35] is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division. It performs analysis on CVEs that have been published to the CVE Dictionary. This analysis is based on impact metrics, such as: Common Vulnerability Scoring System (CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE). Furthermore, NVD uses Security Content Automation Protocol SCAP to deliver catalogues of security vulnerabilities.

Table 1. Current OpenStack vulnerabilities

Vulnerability	Affected component	Type	Confidentiality	Integrity	Availability	CVSS Severity
CVE-2020-8023	Keystone (OpenLDAP)	Acceptance of Extraneous Untrusted Data With Trusted Data	Partial	None	Partial	High
CVE-2020-17376	Nova	Improper Restriction of XML External Entity Reference	Partial	None	None	Critical
CVE-2020-9079	FusionSphere	Failure in protection mechanism	Partial	None	None	High
CVE-2020-10731	Nova	Improper Access Control	Partial	None	None	Critical
CVE-2020-8022	crowbar of SUSE OpenStack	Incorrect Default Permissions	Partial	None	Partial	High
CVE-2020-9225	FusionSphere OpenStack	Improper Privilege Management	Partial	None	None	High
CVE-2018-16848	Mistral service	Uncontrolled Resource Consumption	None	Partial	Partial	Medium
CVE-2020-10755	Cinder	Insufficiently Protected Credentials	Partial	Partial	None	Medium
CVE-2020-12692	Keystone	Missing Encryption of Sensitive Data	Partial	Partial	None	Medium
CVE-2020-12691	Keystone	Missing Encryption of Sensitive Data	Partial	Partial	None	High
CVE-2020-12690	Keystone	Insufficient Session Expiration	Partial	Partial	None	High
CVE-2020-12689	Keystone	Improper Privilege Management	Partial	None	None	High
CVE-2018-17954	crowbar of SUSE OpenStack	Improper Privilege Management	Partial	None	None	High
CVE-2020-9543	Manila version	Incorrect Default Permissions	Partial	None	Partial	High
CVE-2013-7109	Swift	Improper Input Validation	None	Partial	Partial	High
CVE-2015-9543	Nova	Incorrect Default Permissions	Partial	None	Partial	Low
CVE-2019-3683	Keystone	Incorrect Permission Assignment for Critical Resource	Partial	None	Partial	High

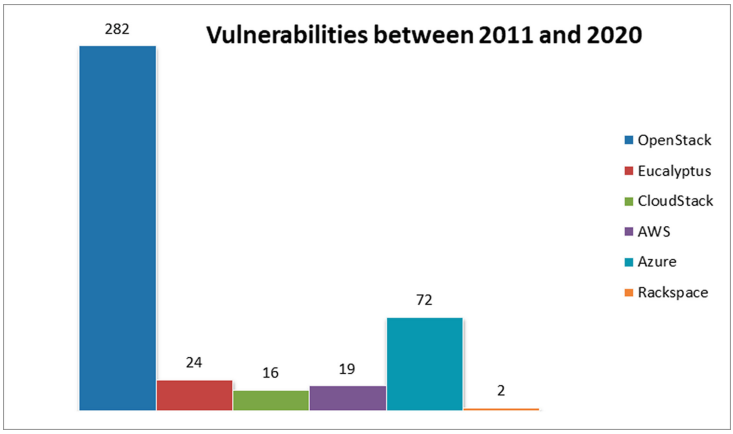

Fig. 4. Vulnerabilities in cloud platforms between 2011 and 2020

Between 2011 and 2019, 282 vulnerabilities have been detected in OpenStack [36]. It is a significant number compared to other platforms, such as: Eucalyptus, CloudStack, Amazon Web Services, Azure, and Rackspace [37] (see Fig. 4).

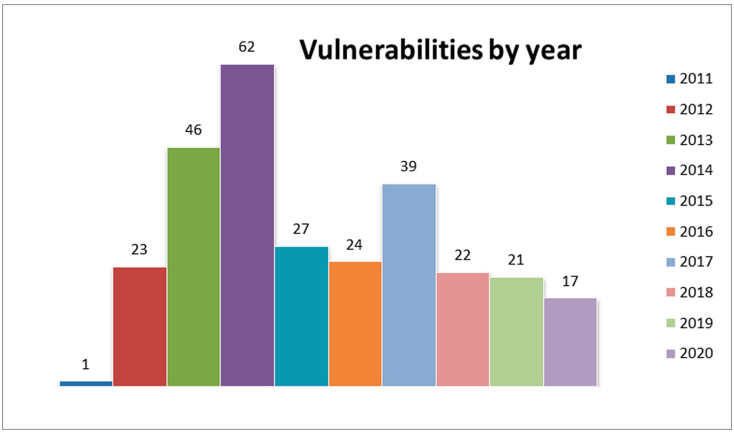

Fig. 5. OpenStack vulnerabilities by year

Moreover, Fig. 5 presents the number of OpenStack vulnerabilities by year. In fact, in 2014, 62 vulnerabilities were detected, while in 2011, Openstack was affected by one vulnerability. Among the 282 Openstack vulnerabilities, 17 have been detected in 2020. In fact, Table 1 detailed the different characteristics of these vulnerabilities. We mentioned the affected component, the vulnerability type, the affected triad CIA, and the CVSS severity. The CVSS is an open

framework for communicating the characteristics and severity of software vulnerabilities. It provides severity ratings ranging from None: 0.0, Low: 0.1–3.9, Medium: 4.0–6.9, and High: 7.0–8.9, to Critical: 9.0–10.0.

Furthermore, as shown in Table 1, Keystone is the most affected component, and most of these vulnerabilities had a high CVSS score and tamper more with data confidentiality rather than integrity or availability. Also, two critical vulnerabilities were affected by Nova component.

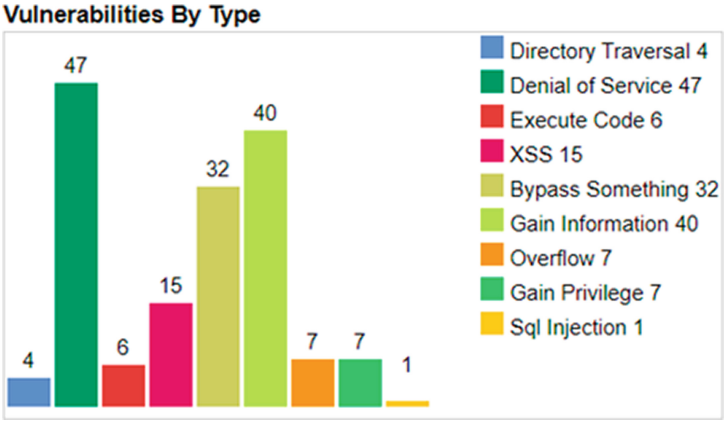

Fig. 6. OpenStack vulnerabilities by type between 2011 and 2020 [34]

Indeed, as shown in Fig. 6, between 2011 and 2019 the most common vulnerabilities were related to DoS (47) followed by vulnerabilities allowing attackers to gain information (40). These vulnerabilities cause serious problems to cloud users and may lead to the emergence of other dangerous attacks. Furthermore, SQL injection vulnerability appeared for the first time in 2019. The vulnerability is founded in ironic function and it could be exploited by attackers to pass malicious data and create a denial of service.

Considering all these statistics, Openstack, as a private cloud management platform, has serious authentication and access control problems; and Keystone is the most vulnerable component. So, researches and studies should give more importance to these issues.

5 Conclusion

OpenStack is an efficient infrastructure as a service platform that delivers solutions for all types of clouds. It is a powerful and highly configurable integration engine. But, it may fail in security concerns. In this paper, we have identified the state of the art of the different components of OpenStack, presented a comprehensive review of the literature, and then analyzed the most common vulnerabilities of OpenStack from 2011 to 2020. From the first detected vulnerability

until today, developers have spent a lot of efforts in fixing a huge number of vulnerabilities. Fortunately, this effort brought to the decrease of vulnerabilities and threats in OpenStack. Currently, just 17 vulnerabilities have been detected in 2020 compared to tens in the last years. These vulnerabilities are related to keystone, Nova, Neutron, Cinder, Swift, and Manilla version. In this work, we provided a comprehensive analysis of the current OpenStack vulnerabilities. We aimed at enhancing the understanding of OpenStack security issues.

References

1. Global Cloud Index Projects: Cloud Traffic to Represent 95 Percent of Total Data Center Traffic by 2021. 05 February (2018)
2. Compound Public Cloud Market Size, Share & Trends Analysis Report By Service (SaaS, IaaS, PaaS), By Enterprise Size (Large Enterprises, SMEs), By End Use (BFSI, Manufacturing), By Region, And Segment Forecasts, 2020–2027. Published Date: May, 2020, Report ID: GVR-4-68038-215-0, Format: Electronic (PDF), 109 p
3. Huang, C., Wang, Y., Li, X., Ren, L., Zhao, J., Hu, Y., Zhang, L., Fan G., Xu J., Gu, X., Cheng, Z.: Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China. Lancet **395**(10223), 497–506 (2020)
4. Tuli, S., Tuli, S., Wander, G., Wander, P., Gill, S. S., Dustdar, S., Sakellariou, R., Rana, O.: Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions. Internet Technol. Lett. **3**(2), e145 (2020)
5. Javaid, M., Haleem, A., Vaishya, R., Bahl, S., Suman, R., Vaish, A.: Industry 4.0 technologies and their applications in fighting COVID-19 pandemic. Diabetes Metabolic Syndrome: Clin. Res. Rev. **14**(4), 419–422 (2020)
6. El Kafhali, S., Salah, K.: Performance analysis of multi-core VMs hosting cloud SaaS applications. Comput. Standards Interfaces **55**, 126–135 (2018)
7. El Kafhali, S., Salah, K.: Modeling and analysis of performance and energy consumption in cloud data centers. Arabian J. Sci. Eng. **43**(12), 7789–7802 (2018)
8. Amazon Web Services AWS: Migrez avec AWS, July 2020. https://aws.amazon.com/fr/
9. Microsoft Azure. Azure est mondial. Azure est local. https://azure.microsoft.com/fr-fr/
10. OpenStack Foundation: OpenStack-Open source software for creating private and public clouds. https://www.openstack.org
11. Eucalyptus community: Eucalyptus is open source software for building AWS-compatible private and hybrid clouds. https://www.eucalyptus.cloud/
12. Apache Software Foundation: Apache Cloudstack - Open Source Cloud Computing, July 2020. https://cloudstack.apache.org/
13. OpenNebula Community: Bringing Real Freedom to Your Enterprise Cloud, July 2020. https://opennebula.org/
14. Gomez-Folgar, F., García-Loureiro, A.J., Pena, T.F., Zablah, J.I., Seoane, N.: Study of the KVM CPU performance of open-source cloud management platforms. In: 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 1225–1228. IEEE, May 2015
15. Vogel, A., Griebler, D., Maron, C.A., Schepke, C., Fernandes, L.G.: Private IaaS clouds: a comparative analysis of OpenNebula, CloudStack and OpenStack. In: 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), pp. 672–679. IEEE, February 2016

16. OpenStack Security Guide. https://docs.OpenStack.org/security-guide/
17. Openstack Horizon, July 2020. https://wiki.openstack.org/wiki/horizon
18. Openstack Nova, July 2020. https://wiki.openstack.org/wiki/nova
19. Jain, P., Datt, A., Goel, A., Gupta, S.C.: Cloud service orchestration based architecture of OpenStack Nova and Swift. In: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2453–2459. IEEE, September 2016
20. OpenStack Neutron, July 2020. https://docs.openstack.org/neutron/latest/
21. Openstack Keystone, July 2020. https://wiki.openstack.org/wiki/keystone
22. Openstack Glance, July 2020. https://wiki.openstack.org/wiki/glance
23. OpenStack Cinder, July 2020. https://docs.openstack.org/cinder/latest/
24. Openstack Swift, July 2020. https://wiki.openstack.org/wiki/swift
25. Luo, Y., Luo, W., Puyang, T., Shen, Q., Ruan, A., Wu, Z.: Openstack security modules: a least-invasive access control framework for the cloud. In: 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), pp. 51–58. IEEE, June 2016
26. Felsch, D., Heiderich, M., Schulz, F., Schwenk, J.: How private is your private cloud? Security analysis of cloud control interfaces. In: Proceedings of the 2015 ACM Workshop on Cloud Computing Security Workshop, pp. 5–16, October 2015
27. Barrowclough, J.P., Asif, R.: Securing cloud hypervisors: a survey of the threats, vulnerabilities, and countermeasures. Secur. Commun. Netw. 20 (2018)
28. Cui, B., Xi, T.: Security analysis of openstack keystone. In: 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 283–288. IEEE, July 2015
29. Madi, T., Majumdar, S., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L.: Auditing security compliance of the virtualized infrastructure in the cloud: application to openstack. In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, pp. 195–206, March 2016
30. Elia, I.A., Antunes, N., Laranjeiro, N., Vieira, M.: An analysis of openstack vulnerabilities. In: 2017 13th European Dependable Computing Conference (EDCC), pp. 129–134. IEEE, September 2017
31. Anisetti, M., Ardagna, C.A., Damiani, E., Gaudenzi, F.: A security benchmark for openstack. In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), pp. 294–301. IEEE, June 2017
32. Gordin, I., Graur, A., Potorac, A., Balan, D.: Security Assessment of OpenStack cloud using outside and inside software tools. In: 2018 International Conference on Development and Application Systems (DAS), pp. 170–174. IEEE, May 2018
33. Hogan, K., Maleki, H., Rahaeimehr, R., Canetti, R., Van Dijk, M., Hennessey, J., Varia, M., Zhang, H.: On the universally composable security of openstack. In: 2019 IEEE Cybersecurity Development (SecDev), pp. 20–33. IEEE, September 2019
34. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. https://www.cvedetails.com/
35. NVD National Vulnerability Database, September 2020. https://nvd.nist.gov
36. NIST, National Vulnerability Database, September 2020. https://nvd.nist.gov/vuln/search
37. Rackspace: End-to-End Multicloud Solutions, September 2020. https://www.rackspace.com/