Towards Vulnerability Assessment as a Service in OpenStack Clouds

Kennedy A Torkura and Christoph Meinel Chair of Internet Technologies and Systems Hasso Plattner Institute, University of Potsdam Potsdam, Germany Email: {kennedy.torkura, christoph.meinel}@hpi.de

Abstract—

Efforts towards improving security in cloud infrastructures recommend regulatory compliance approaches such as HIPAA and PCI DSS. Similarly, vulnerability assessments are imperatives for fulfilling these regulatory compliance requirements. Nevertheless, conducting vulnerability assessments in cloud environments requires approaches different from those found in traditional computing. Factors such as multi-tenancy, elasticity, self-service and cloud-specific vulnerabilities must be considered. Furthermore, the Anything-as-a-Service model of the cloud stimulates security automation and user-intuitive services. In this paper, we tackle the challenge of efficient vulnerability assessments at the system level, in particular for core cloud applications. Within this scope, we focus on the use case of a cloud administrator. We believe the security of the underlying cloud software is crucial to the overall health of a cloud infrastructure since these are the foundations upon which other applications within the cloud function. We demonstrate our approach using OpenStack and through our experiments prove that our prototype implementation is effective at identifying "OpenStacknative" vulnerabilities. We also automate the process of identifving insecure configurations in the cloud and initiate steps for deploying Vulnerability Assessment-as-a-Service in OpenStack.

Index Terms—Cloud-security, vulnerability assessment,Security as a Service, cloud-specific vulnerabilities

I. INTRODUCTION

Cloud computing landscape is witnessing a dramatic phase. There is a growing adoption of private Infrastructure as a Service (IaaS) clouds, as the security of this cloud model offers more guarantees than public clouds. Almost every major Cloud Service Provider (CSP) offer a kind of "private cloud", yet there is a preferrence among enterprises for either a hosted private cloud or an "on-premise" private cloud. RightScale [1] asserts that OpenStack and VMware are the leading private cloud vendors. OpenStack [2] offers an open source cloud computing software while VMware [3] provides a proprietary and commercial cloud computing suite. Benefitting from the innovativeness of open-source software, OpenStack has beome a very popular option for private cloud. OpenStack offers almost every service available on commercial clouds such as Amazon Web Services (AWS). However, several challenges hinder OpenStack adoption, accordingly the number of production-level deployments is not commensurate with its popularity. The lack of sufficient security assurances largely contribute to this lapse[4]. Several factors militate against security in OpenStack. It's ecosystem is complex, consisting of over then 15 projects (which could be either installed independentaly/semi-independentaly). Deploying a full stack cloud requires multiple levels of configuration across these services, this introduces misconfigurations. Furthermore, the bi-yearly release circle is a challenge for maintaining stable and current deployments [4]. Every release includes changes in configurations, packages are either deprecated or modified and sometimes new services are introduced. Since there are no provisions for automated upgrades, maintaining current releases introduces security issues. Moreso, there is no integrated vulnerability assessment tool for identifying these security issues.

Existing research in the scope of OpenStack vulnerabilities identify some of these security challenges yet solutions are hardly proffered. The OpenStack security team maintains resources which could be leveraged to improve a good number of these security challenges. However, these resources have low publicity and suffer from lack of automated approaches/tools. But automation is a key requirement in cloud security [5] and it is critical for regulatory compliance. Similarly, several attempts at standardizing the security in the cloud recommend vulnerability assessment as an important activity [6].

The Cloud Security Alliance (CSA) specifies implementation guidelines for Security-as-a-Service (SecaaS) including its sub-categories such as Vulnerability Assessment-as-a-Service (VAaaS), Monitoring as a Service (MONaaS) and Firewallas-a-Service (FWaaS). We are more concerned with VAaaS considering its requirement for compliance regulations. Hence, in this work we introduce approaches for designing and employing VAaaS in OpenStack. Our focus is on the system level vulnerabilities from a cloud administrator perspective. We consider vulnerabilities native to OpenStack core software, best practices recommended by the OpenStack security team and how these security provisions can be automated and integrated into a vulnerability assessment system. Hence we designed and implemented Cloud Aware Vulnerability Assessment System (CAVAS), a prototype system that resolves the mentioned security challenges.

Our major contributions are as follows:

• We introduce an approach for integrating vulnerability

© 2016, Kennedy A. Torkura. Under license to IEEE. DOI 10.1109/LCNW.2016.15 1



assessment in OpenStack especially at the system level, suitable for cloud administrators.

- Integration of our previously introduced approach [7] for reducing the "window of opportunity" (for vulnerability exploitation) introduced by late release of security patches.
- We present an automated approach for conducting security checks through the use of security policies and security best practices that are recommended by OpenStack security team.
- We briefly survey the state-of-art in cloud vulnerability assessment.

In the next Section, we consider the works that are similar to ours. In Section III, we briefly investigate the current security projects in OpenStack and highlight the challenges in ensuring effective vulnerability assessments. Next, in Section IV we discuss the state-of-the-art in cloud vulnerability assessment by considering current strategies deployed by leading CSPs and third-party SecaaS vendors. Drawing from the aforementioned, we introduce our VAaaS approach in Section V. In Section VI, we evaluate our work and highlight our next steps in Section VII. We conclude the paper in Section VIII.

II. RELATED WORK

We identified two research areas that are related to our work, research in the area of cloud vulnerability assessment and risk management, and research focusing on evolving SecaaS frameworks.

The challenges of risk management and vulnerability assessments in the cloud were investigated in [8]. The authors provided useful research directions for overcoming these challenges, however there is no practical implementation validating their recommendations. We implemented some of these recommendations in our work. Ristov et al [9] conducted a security assessment of the OpenStack cloud from within the cloud and from outside the cloud environment. In their work, they evaluated the vulnerabilities that exist in OpenStack cloud tenants. However, the security of the core OpenStack services and system vulnerabilities was not covered. In this work we focus on vulnerabilities that affect the core OpenStack services. Kamongi et al [10] introduced an approach for cloud vulnerability assessment that employs security ontology knowledge-bases for risk and threat mitigation. The same authors extend their work in the NEMESIS framework [11] however, we opine that their approaches might not be effective in discovering "OpenStack-native" vulnerabilities since they rely on vulnerability scanners that do not adequately include vulnerability information regarding OpenStack.

In [12], the authors introduced "Potassuim", a framework that leverages OpenStack services and APIs for penetration testing. "Project Mirroring" approaches are used to capture the live state of running cloud environments. Third party security tools like the MetaSpoit framework are integrated into "Potassium". The efficiency of this system would be enhanced with OpenStack-native security tools like the one presented in this paper. Almorsy et al's [13] work is closest to ours, formal approaches are employed for specifying vulnerability signatures in web applications. This work differs from ours in that we target system-level vulnerabilities based on disclosed vulnerabilities and best practices. We also apply our framework to a specific cloud environment and demonstrate its feasibility.

On a more general note, the major difference between our work and existing ones is our focus on integrating vulnerability assessment into OpenStack . We evolve novel ways specifically targeted at "OpenStack-native" vulnerabilities to enhance the efficiency of security assessments. This is inline with Grobauer assertion [14] on the need to differentiate between general vulnerabilities and cloud-specific vulnerabilities.

III. STATE OF SECURITY IN OPENSTACK: CHALLENGES AND PROSPECTS

OpenStack is an open-source cloud computing software [15] developed and maintained by a large community of developers. In this section, we briefly describe OpenStack's architecture, the current security structure and the challenges to secure deployments.

A. OpenStack Mitaka Architecture

OpenStack Mitaka is the latest release of OpenStack, several new features were introduced with Mitaka but those directly impacting on security include time-based one time password, implied roles and unified identity for multiple authentication sources. OpenStack has a modular structure consisting of several services, the main ones are: swift (object storage), keystone (identity service), horizon (user interface), nova (compute), cinder (Virtual Machine (VM) storage) and glance (VM catalog service).

B. Security and Vulnerability Management in OpenStack

The OpenStack security project consists of an OpenStack Security Team and a Vulnerability Management Team (VMT). The security team's responsibilities include production of security notes and developer guidance documents [16].

The OpenStack VMT is responsible for effective handling of vulnerabilities affecting OpenStack. The VMT has adopted coordinated vulnerability disclosure approach, a middle-ground between full disclosure and non-disclosure approaches. Hence, information about newly discovered vulnerabilities is initially restricted to a small number of OpenStack security developers. Following, a specific vulnerability management procedure [17], the downstream stakeholders are informed through secure channels. This step is critical since OpenStack is an upstream project deployed by several downstream vendors which could be adversely affected by inappropriate disclosure of vulnerabilities. Accordingly, these stakeholders are forewarned of vulnerabilities to ensure smooth patch development and deployment.

C. OpenStack Security Projects

In order to understand the security posture of OpenStack, an insight into existing security projects [16] maintained by

Vendor	Supported Host OS	Automation/Orchestration Tool	Security Schemes
OpenStack	Ubuntu, Fedora, RedHat and CentOS	DevStack, Manual installation from OpenStack repository	OpenStack Security Advisories (OSSA), OpenStack Security Notes (OSSN) and OpenStack Security Guide
Mirantis	Ubuntu, Fedora, OpenSuse, MacOS, Windows (with Cygwin)	Fuel and Puppet	Fuel plugins for security monitoring, Firewall-as-a-Service (FWaaS), Bug tracking/fixing
Oracle	Oracle Linux	Docker-based and Ansible	None
RedHat	RHEL	OSP Director (Tripleo), PackStack (RDO)	Monitoring with Nagios ,Bug tracking/- fixing
Suse	Suse Linux Enterprise Server	Crowbar, Chef	None
Ubuntu	Ubuntu Linux	Landscape, MAAS and Juju	Bug tracking/ fixing

Table I: OpenStack Vendors and Deployment Strategies

the Openstack Security team is imperative. These are: Open-Stack Security Notes (OSSN), OpenStack Security Advisories (OSSA), Anchor, and Bandit. OSSN and OSSA are basically security information initiatives aimed at retaining the current information about vulnerabilities. OSSN contains information on third party applications and security best practices such as configurations. On the other hand OSSA like other security advisories, are documents published to disclose information on discovered vulnerabilities. Anchor is a lightweight facility for managing cryptographic certificates, while Bandit is a code linter for Python. The above mentioned security projects are more suited for core OpenStack developers, they do not fit the security needs of normal users or cloud administrators. These projects are neither automated nor modelled after Anythingas-a-Service (XaaS) as requirred for cloud environments. If designed according to the XaaS model such as other Open-Stack services e.g. MONaaS [18] and FWaaS, the benefits of these tools could have wider coverage.

D. Lapses and Complexity in Vulnerability Management

Despite its popularity, OpenStack is still considered as a complex software. Firstly, OpenStack has a modular structure consisting of over 15 services. Secondly, almost every Linux distribution supports and maintains distribution-specific OpenStack packages. Thirdly, OpenStack's major releases are unveiled every six months with several changes in the cloud stack including performance improvements and security fixes [19]. While it might be a best practice to upgrade deployments inline with major releases, the upgrade procedure is majorly manual since there is no provision for automated upgrading. This creates opportunities for risks owing to human errors and mis-configurations [4]. Hence, in reality productive deployments hardly maintain the current stable releases. In order to tackle these complexities, vendors employ various automated orchestration strategies as shown in Table 1. Automation is a key feature in cloud environments, however the security implications of adopting these tools ought to be evaluated. For example, automated tools could expose cloud deployments to risks such as changes to roles and privileges and modification of critical files[20]. OpenStack's multi-vendor approach requires a well coordinated vulnerability management strategy, one that properly handles vulnerabilities discovery, vulnerability disclosure and patch release across upstream

and downstream vendors. This is not available in the current vulnerability management strategy, for example there is no centralized source of vulnerability information for OpenStack clouds where vulnerabilities discovered by the various vendors is documented.

IV. STATE OF THE ART APPROACHES IN CLOUD VULNERABILITY ASSESSMENT

Security in the public cloud is a shared responsibility [21], CSPs ensure security at the infrastructure level while cloud customers are responsible for security of their data, applications, OSs and networks. However, cloud customers are limited in the types of security tools they can employ in fulfilling their own part of this responsibility. Owing to multi-tenancy, most CSPs enforce a requirement on customers for prior permission before conducting vulnerability assessments and penetration testing. Alternatively, an evolving approach is the provision of SecaaS by CSPs. Nevertheless, customers are not limited to these services, employment of third-party SecaaS is also permissible. There are currently several flavors of this service especially in the area of web application scanners. SecaaS aims at leveraging on cloud characteristics to empower cloud users to satisfy security requirements at a low cost in terms of finances and human resources. The efficiency of the current SecaaS services is yet to be properly scrutinized, most of the vendors migrated their security approaches to the cloud from traditional computing environments with little or no consideration of the peculiar nature of cloud environments. In the following subsections, we consider some of these vendors and briefly describe their services. We do not aim at comparing the efficiency of these security services but to highlight the current state-of-the art in cloud vulnerability assessment.

1) Amazon Inspector: Amazon Inspector [22] is an automated security assessment service provided on the AWS cloud platform. Just like other services available on AWS cloud, it is provided as a service, following the SecaaS model. Amazon Inspector leverages on a knowledge-base of rules that are mapped to common security issues and best practices. These rules are regularly updated by the AWS security team and include support for popular security metrics like the Common Vulnerability Scoring System (CVSS). Using these rules, users can launch and deploy agents on target instances to scan and identify security lapses in applications, databases and other resources. Amazon Inspector is accessible via AWS APIs, SDKs, command line tools and AWS management console. The core of Amazon Inspector are the rules which conduct the actual scanning. Each rule is assigned a security level to aid in assessing the severity of a security issue; high, medium, low and informational. These rules are available in four categories;

- Common Vulnerabilities and Exposures
- Centre for Internet Security (CIS) Operating System Security Configuration Benchmarks
- Security Best Practices
- Runtime Behaviour Analysis

2) Google Cloud Security Scanner: Google Cloud Security Scanner ¹ is a Web Application Scanner available on the Google Cloud platform. It currently supports only applications hosted on Google App Engine, application developers especially can use it as a service to secure their applications. It is still in beta as at the time of this writing and covers a small variety of web application vulnerabilities such as crosssite scripting and mixed content. Users are therefore advised to compensate this scanner with other scanners to further secure their applications. The Google Security Scanner employs several chrome workers and Google Compute Engines instances to horizontally scale to the required scan load. Just like other web applications, follows links and urls and employs the use of simulated user inputs and event handlers.

3) Third Party Vulnerability Assessment Vendors: There is a large number of third party Vulnerability Assessment Vendors. While some of these vendors evolved their services for traditional security services, some of them are relatively new. They offer various kinds of SecaaS opportunities including vulnerability assessments, monitoring and threat mediation. Some vendors have their images deployed on public clouds, and partner with the respective CSPs for tight cloud security integration. There are several advantages for using this services, for example customers may not be required to request for prior permission to perform vulnerability assessment against resources on AWS if such security operations are conducted via SecaaS partners like AlertLogic and Nessus [23]. Yet, assessments though these providers is limited to some resources. For example, Relational Database Service (RDS) instances cannot be scanned on AWS cloud platform. the other category of cloud vulnerability services offer their services such that they can be directed against resources deployed in public clouds. The key requirements for these vendors is that subscribers provide some form of credentials for "credentialed scans" for example they may create a non admin role on their cloud dedicated to vulnerability scanning. Scanning results can also be saved on a cloud-database such as AWS Simple Storage Service (S3) or exported to a customer preferred location. They are also able to scan across security groups and databases on a scheduled timetable or on a one-off setting.

V. INTEGRATING A VULNERABILITY ASSESSMENT FRAMEWORK INTO OPENSTACK

OpenStack does not currently offer an integral vulnerability assessment service. While it is possible for third party assessment tools to be used for vulnerability assessments and auditing, integrated tools offer cloud-native approaches and results. Third-party tools could be limited by CSPs from auditing multi-tenant resources such as hosted databases, the dynamic nature of cloud resources e.g. elastic ip addressing also presents a challenging situation. Such limitations reduce the level of control a CSPs ought to have. Hence, as discussed in Section III, the current approach in cloud vulnerability assessments consists in CSPs offering VAaaS on their platforms. These approaches to vulnerability assessments are designed to be flexible, cheap in cost and easy to use, just as other cloud services. The advantages are similar to those of other cloud services such as ease of use while hiding the complexities of security configurations behind the scenes. VAaaS is also applicable to enterprise private clouds where employees can effectively assess their resources without requiring the normal "technical knowledge". This reduces the burden from the security staff and promotes security in the enterprise. We opine that integrating a VAaaS into OpenStack is an important component for OpenStack security. The basic requirement for a vulnerability assessment tool suitable for integration into OpenStack would be that it is open-source and supports Linux distributions. We considered several open-source vulnerability assessment tools and eventually selected Open Vulnerability Assessment System (OpenVAS). OpenVAS is a fork of the popular Nessus vulnerability scanner. It consists of several security tools suited for vulnerability scanning and assessment, it has features that are commonly found in commercial products. OpenVAS is commonly used for security research. It is suitable for different levels of vulnerability-related tasks such as Local Security Checks and network scanning. We have integrated OpenVAS into OpenStack using our system called CAVAS. Most components of CAVAS are implemented in Java, more details on our implementation is provided in the next sections. Note that we have focused on vulnerabilities affecting the core OpenStack software and applications. We are not concerned with the vulnerabilities that affect the other applications such as web applications and databases. We feel that the existing vulnerability assessment tools are quite mature for the task of traditional applications.

A. Aggregating and Adapting Vulnerability Information for OpenStack

Vulnerability scanners heavily rely on information about existing or discovered vulnerabilities [24], such information is acquired from various sources including the National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB) and SecurityFocus². While information from these sources suffice for assessing traditional systems, information

¹https://cloud.google.com/security-scanner/

²http://www.securityfocus.com/



Figure 1: Architecture of CAVAS.

regarding cloud-specific vulnerabilities is requisite for assessing core OpenStack software components such as keystone and swift. In order to acquire these specific information, an approach that targets and captures this information is imperative. Hence, in order to satisfy these requirements, we adopt a two step approach:

1) Vulnerability Information from External Sources: In the first step, we gather information from outside OpenStack. We leverage on Hasso Plattner Institute Vulnerability Database (HPI-VDB) ³, a vulnerability database developed and maintained by the Hasso Plattner Institute (HPI) security research team. It retains over 75000 vulnerabilities extracted from various sources including the NVD, OSVDB and SecurityFocus.

2) Vulnerability Information from Internal Sources: The second step involves aggregation of information from sources within OpenStack, more specifically from the OSSN, OSSA and OpenStack Launchpad Bug-tracker (OLB). OSSN and OSSA are security initiatives maintained by OpenStack security team to keep OpenStack downstream stakeholders and users abreast with security information [25]. OSSN contains updated information about security best practices such as secure configurations. We also observed that several security issues are not mitigated but proposed for implementation in future releases. Also, approaches for mitigating these security issues are described in OSSN. However, the awareness of these information sources is sparse, and OpenStack provides no automated tools for easily consumption of these information. Moreso, the downstream stakeholders selectively use the information according to their requirements i.e. only when it concerns their product. Similar to the security notes, OSSA contains detailed information about vulnerabilities discovered. However, the information at OSSA covers core OpenStack services. The last source of our vulnerability information is the OLB, which is retained on LaunchPad. We include this as an internal information source because it is heavily used for development-related communication within Open-Stack development teams and OpenStack vendors. Similar to the previously mentioned sources, the awareness of the information available at OLB is limited, infact most people aware of this source are software developers. However, information derived from OLB is very useful and could be used to improve security. We extend the functionality of our previously



Figure 2: Screenshot of Search Result in OpenVAS Plugins Database Showing CVE-2015-3241 not found.

published paper [7] which detailed a framework for leveraging information from OLB. The framework demonstrated the use of information derived from OLB for reducing the "window of opportunity" for exploiting security holes in software. Accordingly, we have integrated security-related information extracted from OLB into CAVAS.

B. Components of the Our Scheme - Cloud Aware Vulnerability Assessment System (CAVAS)

1) Vulnerability Information Aggregator: The architecture of CAVAS is shown in Figure 1. As shown in the architecture, the Vulnerability Information Aggregator is responsible for collecting information from the sources mentioned in the previous sub-section. We collect information from sources internal and external to OpenStack as described in the previous sub-section. Different approaches are adopted to achieve this objective, depending on the specific source. For example, information from HPI-VDB is collected via a REST interface, while the OSSA git repository is cloned from OpenStack GitHub repository ⁴ and thereafter parsed into our local MongoDB database. We prefer MongoDB since it supports schema-less database structure, which is suitable for storing vulnerability information [26].

2) Vulnerability Information Processor: The data retrieved from the various sources contains several pieces of information, however we are interested in specific content such as the vulnerability title, vulnerability description, Common Vulnerabilities and Exposures (CVE) identifier, CVSS base score, affected products and availability of a fix. We employ our "custom extraction algorithm" for extracting and collating these pieces of information. For each vulnerability entry, we aim at collating information that represents a comprehensive picture of the specific vulnerability suitable for plugin generation.

3) Vulnerability Correlator: During our previous work on vulnerability life-cycles [27], we realized a gap between when vulnerabilities are publicly announced, when fixes are released by respective vendors and when security tools especially vulnerability scanners develop appropriate plugins to identify these vulnerabilities. We characterized these findings as *Scanner Patch Time* and *Scanner Patch Discovery Time*. These issues are still evident in OpenStack for example, we developed a plugin for CVE-2015-3241 since there was none available in the OpenVAS plugin repository (Figure.2). These plugins are scripts that test target systems for specific vulnerability issues. The Vulnerability Correlator compares the

⁴https://github.com/openstack/ossa

³https://hpi-vdb.de/vulndb/

information acquired in the last step with the plugins in the local OpenVAS plugin repository. This step is important to prevent duplicate plugins. Vulnerabilities lacking plugins are then queued for development in the next step.

4) Plugin Generator: The plugin generator automatically constructs the required plugins as determined in the previous step. Vulnerability signature generation has been used in previous security research such as Intrusion Detection Systems (IDS) [28] and anti-virus systems, we gain inspiration from these efforts but apply similar approaches to vulnerability assessment. The plugins are developed in Nessus Attack Scripting Language (NASL), a scripting language used for OpenVAS and Nessus Scanner. Automatic development of these plugins minimizes human intervention and aids timely production of plugins in response to discovered vulnerabilities. We utilize the templating capabilities of Apache Freemarker Templating framework ⁵ to generate two types of plugins: Local Security Checks and Policy Checks. The Local Security Checks are constructed using information derived from HPI-VDB, OSSA and OLB. These checks test target systems for specified vulnerabilities already discovered and published. On the other hand, Policy Checks are derived based on information extracted from OSSN. These checks may not necessarily search for existing vulnerabilities, rather they verify if best practices recommended by the OpenStack security team are being applied on the target system. These policies also check for configuration errors.

5) Scanner Module: The scanner module is the hub of our system. We leverage on OpenVAS scanner for our framework rather than designing and developing a scanner from the scratch. OpenVAS has a modular structure consisting of OpenVAS scanner, OpenVAS manager, a Command Line Interface (CLI) and a web client. Hence it is feasible to extend the existing functions of any of these modules. Through the use of the the XML-based OpenVAS Management Protocol (OMP), CAVAS executes scan commands to the scanner. OMP supports automation of batch processes which, we have leveraged on this feature in our work.

VI. EVALUATION

We have conducted a set of experiments to evaluate the suitability of our prototype implementation. Here, we describe these experiments and provide the results we obtained. Experiments were conducted against a target OpenStack cloud environment. Since the focus of these initial steps is to validate our approach from a cloud administrator perspective, we deployed a basic OpenStack cloud environment as the target. The target environment is an OpenStack Icehouse environment installed on Windows Laptop with the following configuration : Intel i5, dual core CPU and 12GB memory.

We conduct two category of tests, in the first category we aim at identifying vulnerabilities while the second tests are designed to spot mis-configurations based on our security policy checks. Our security policy checks are aimed at identifying

⁵http://freemarker.org/

Uburtlu update for ganti26 USN-2913-4 10.0 X ✓ Ibgrufts Uburtlu update for ganti26 USN-2913-1 10.0 X ✓ OpenSIS. C Uburtlu update for accentificates USN-10.0 X ✓ OpenSIS. C C Uburtlu update for accentificates USN-10.0 X ✓ OpenSIS. CVE-2016-0702. CVE-2016-0705. Uburtlu update for rAM USN-291-1 10.0 X ✓ Belgap. CVE-2017-4708 Uburtlu update for rabults values account of the gantiticate structures account on rabults values account of the gantiticates account on rabults values account on rab	Ubuntu update for gnuti26 USN-2913-4 Ubuntu update for general USN-2913-4 Ubuntu update for co-entificates Ubuntu Update for Co-entificates Ubuntu Update for Bibliogn USN-291-1 Ubuntu Update for Bibliogn USN-295-1 Ubuntu Update for Bibliogn USN-295-1 Ubuntu Update for Bibliogn USN-2918-1 Beitze/dalete combo allows to overload novo-compute Nova may fail to delete images in resize Glance tixoge quicto byposs when token is expired	10.0 10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x x	· · · · · · · · · · · · · · · · · · ·	Ibgnutts OpenSSL CA-Certificates OpenSSL Iktasp gemu-system-x86	CVE2016-0702, CVE2016-0705, CVE2016-0708, CVE2013-7422, CVE2016-2881 CVE2013-7422, CVE2014-2894
Ubuntu update for gruti224 USN-2913-4 10.0 X ✓ Bigurufts Ubuntu update for appenditudes USN- 2013-4 10.0 X ✓ Open531. Ubuntu update for appenditudes USN- 2013-4 10.0 X ✓ Open531. CVE-2016-0702. <	Ubuntu update for grunti26 USN-2913-4 Ubuntu update for garsat USN-2913-3 Ubuntu update for garsat USN-2913-3 Ubuntu update for PAN USN-2914-1 Ubuntu Update for PAN USN-2914-1 Ubuntu Update for PAN USN-2914-1 Ubuntu Update for gattus -2916-1 Ubuntu Update -2916-1 Ubuntu Update -2916-1 Ubuntu Update -2916-1 Ubuntus -2916-1 Ubuntu Update -2916-1 Ubuntus -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1 -2916-1	10.0 10.0 10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x x	× · · · · · · · · · · · · · · · · · · ·	Ibgnutts OpenSSL CA-Certificates OpenSSL Iblaso gemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-0708, CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2384
Ubuntu update for grutus2 USN-2913-4 10.0 X ✓ Bigmuts Ubuntu update for grutus2 USN-2913-4 10.0 X ✓ OpenStit Ubuntu update for grutus2 USN-2913-4 10.0 X ✓ OpenStit CA-Certificates Ubuntu update for scheartificates USN-1 10.0 X ✓ CA-Certificates Upuntu Update for grutus USN-2914-1 10.0 X ✓ CA-Certificates Upuntu Update for grutus USN-2914-1 7.3 X ✓ Restrict ALL CVE-2016-4008 Ubuntu Update for grutus USN-2914-1 7.3 X ✓ genur-system-366 CVE-2016-4026 CVE-2016-42081 Ubuntu Update for grutus USN-2916-1 7.3 X ✓ genur-system-366 CVE-2016-42081 CVE-2016-42081 Ubuntu Update for grutus USN-2012-1 7.2 X ✓ genur-system-366 CVE-2016-42081 Restrict Alexit CVE-2012-1 7.2 X ✓ genur-system-366 CVE-2015-5281 Nova movindo for degrutus Uspate 6.8 ✓ X OpenStack Nova CVE-2015-5280 Glonce v2	Ubuntu update for grunti26 USN-2913-4 Ubuntu update for general UBN-2913-4 Ubuntu update for co-certificate USN- 2913-4 Ubuntu Update for Abu USN-2914-1 Ubuntu Update for ablags USN-295-1 Ubuntu Update for gamu USN-2916-1 Ubuntu Update for gamu USN-2182-1 Babiz/date/comba devento overload novo-compute Novo may rafi to detete images in resize Clance expred	10.0 10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x x x	* * * *	Ibgnutts OpenSSL CA-Certificates OpenSSL Iblast, gemu-system-x86	CVE2016-0702, CVE2016-0705, CVE2016-4008 CVE2013-422, CVE2016-2381 CVE2013-4544, CVE2014-2894
Uburnu update for grunit2 UBX-2913-4 10.0 X ✓ Ibigrafits Uburnu update for general UBX-2913-4 10.0 X ✓ Open531 CAC Extificates Uburnu Update for general UBX-2913-1 10.0 X ✓ Open531 CAC Extificates Uburnu Update for FAM UBX-2914-1 10.0 X ✓ Open531 CVE-2016-4006 Uburnu Update for Batta UBX-291-1 7.0 X ✓ Ibidary CVE-2013-4242 CVE-2016-4006 Uburnu Update for gengy UBX-292-1 7.2 X ✓ genu-system 366 CVE-2013-4244. CVE-2016-42081 Uburnu Update for gengy UBX-292-1 7.2 X ✓ genu-system 366 CVE-2013-4244. CVE-2016-42081 Uburnu Update for gengy UBX-292-1 7.2 X ✓ genu-system 366 CVE-2013-3242. CVE-2016-42081 Betzer/delete combo allows to overfold on accompte 6.8 ✓ X Open510ck Nova CVE-2015-3280 Glance storage quoto bypass 6.8 ✓ X Open510ck Keystone CVE-2015-3286. CVE-2015-3280.	Ubuntu update for ganufizik UISN-2913-4 Ubuntu update for ganagi UISN-2913-4 Ubuntu update for ca-certificates UISN- Ubuntu Update for 2A-certificates UISN- Ubuntu Update for RIMAR UISN-2914-1 Ubuntu Update for RIMAR UISN-2915-1 Ubuntu Update for gampu UISN-2182-1 Ubuntu Update for gampu UISN-2182-1 Ubuntu Update for gampu UISN-2182-1 Ubuntu Update for gampu UISN-2182-1 Nova may fait I delete images in resize uben tokan is expired	10.0 10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x x	× × × × × × × ×	libgnuttis OpenSSL CA-Certificates OpenSSL Ibbass, gemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Ubuntu update for opensal USH-2913-3 10.0 X ✓ OpenSt. Ubuntu update for op-certificater USH-2013-3 10.0 X ✓ CA-Certificater Ubuntu update for PAM USH-2914-1 10.0 X ✓ CA-Certificater Ubuntu Update for PAM USH-2914-1 10.0 X ✓ OpenStL CVE-2016-4705, CVE-2016-4705, UVE-2016-4705, UVE-2016-4704	Ubuntu update for opensii USN-2913-3 Ubuntu update for co-certificates USN- 2913-4 Ubuntu Update for PAM USN-2914-1 Ubuntu Update for PAM USN-2915-1 Ubuntu Update for gentu USN-2916-1 Ubuntu USN-2916-1 Ubuntu USN-2916-1 Ubuntu USN-2916-1 Ubuntu USN-2916-1 Ubuntu Update for gentu USN-2916-1 Ubuntu USN-2916-1 Ubuntu USN-2916-1 Ubuntu Update for gentu USN-2916-1	10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x	* * * * *	OpenSSL CA-Certificates OpenSSL Iblash gemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Uburnu update for <u>persons</u> (BN-2913-3) 10.0 X ✓ OpenState Uburnu update for <u>persons</u> (BN-2913-3) 10.0 X ✓ OpenState Uburnu update for <u>persons</u> (BN-2914-4) 10.0 X ✓ OpenState CVE-2016-0702, CVE-2016-0702, CVE-2016-0705, CVE-2016-0705, CVE-2016-0705, CVE-2016-0705, CVE-2016-0705, CVE-2016-0705, CVE-2016-0706, CVE-201	Usunit update for <u>spans</u> (USX-201-3). Usunit update for ca-certificates USX- Ubunit update for CA-certificates USX- Ubunit update for RIMUSX-291-11 Ubunit Update for <u>RIMUSX-291-3</u> Ubunit Update for <u>active</u> USX-2182-11 Retaite/delete combo allows to overfoad novo-compute Nova may fail in delete images in resize use torage quale bypas when token is expired	10.0 10.0 10.0 7.5 7.2 6.8 6.8	x x x x x x	✓ ✓ ✓ ✓ ✓ ✓	OpenSSL CA-Certificates OpenSSL Ibtasa, gemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Uburtu update for co-certificates UN- 2013. 10.0 X ✓ CA-Certificates Uburtu Update for PAM USN-291-41 10.0 X ✓ OpenStit. CVE-2016-0702, CVE-2016-0705, USN-2012-17, S X ✓ OpenStit. CVE-2016-0702, CVE-2016-0705, USN-2012-17, S X ✓ OpenStit. CVE-2016-0702, CVE-2016-0705, USN-2012-17, S X ✓ OpenStit. CVE-2016-4008 CVE-2016-4008 Uburtu Update for gentu USN-2182-1 7.2 X ✓ genu-pytem-x86 CVE-2016-4281 CVE-2016-4281 Board nova-compute 6.8 ✓ X OpenStack Nova CVE-2016-3280 Conce storage quotes byoars 6.8 ✓ X OpenStack Nova CVE-2015-3280 Conce storage quotes byoars 6.8 ✓ X OpenStack Keystone CVE-2015-3280 Conce storage quotes byoars 6.8 ✓ X OpenStack Keystone CVE-2015-3280 Uburtu Update for PAM USN-2235-2 5.8 X ✓ Ibparm-modules CVE-2015-3280, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, CVE-3013-328, C	Ubunit update for co-certificates USH- 2913-4 Ubunit Update for PAM USN-2914-1 Ubunit Update for page USN-2916-1 Ubunitu Update for gamy Update for gamy Ubu	10.0 10.0 7.5 7.2 6.8 6.8	x x x x x	✓ ✓ ✓ ✓ ✓	CA-Certificates OpenSSL libtasn qemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-4008 CVE-2018-7422, CVE-2016-2381 CVE-2013-7422, CVE-2014-2894
Upuntu Update for PAM UBN-291-1 10.0 X ✓ Open53L CVE-2016-0702, CVE-2016-0705, CVE-2016-0705	Ubunt Update for PAM USN-2914-1 Ubunt Update for PAM USN-2914-1 Ubunt Update for <u>plana</u> , USN-2957-1 Ubuntu Update for <u>patty</u> , USN-2182-1 Ubuntu Update for <u>patty</u> , USN-2182-1 Ubuntu Update for <u>patty</u> , USN-2182-1 Nava may fail to delete images in resize Glance storage quote bypas when token is expired	10.0 10.0 7.5 7.2 6.8 6.8	x x x x	✓ ✓ ✓ ✓	OpenSSL libtasn gemu-system-x86	CVE-2016-0702, CVE-2016-0705, CVE-2016-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Uburn Update for FAN USA-21-1 U.U. X C pensit CVF2014 SUZ, CVF2014 SUZ	Usuntu Update for PAN USX-214-1 Ubuntu Update for gatu USX-235-1 Ubuntu Update for gatu USX-2316-1 Ubuntu Update for gatu USX-2316-1 Ubuntu Update for gatu USX-2316-1 Ubuntu Update for gatu USX-2316-1 Ubuntu Update for gatu USX-2316-1 Nove may fall to detete images in resize babe Clance storage quote bypas when token is expired	10.0 10.0 7.5 7.2 6.8 6.8	x x x x	✓ ✓ ✓ ×	apenu-system-x86	CVE-2018-0702, CVE-2018-0705, CVE-2013-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Tubuntu budate for jaban. 198-295-71 10.0 X -/ jaban. CVF-2015-4008 Ubuntu budate for gatty. USA-2182-11 7.3 X -/ genu-system.x85 CVF-2015-4208 Ubuntu budate for gatty. USA-2182-11 7.3 X -/ genu-system.x85 CVF-2015-4224 Vestoria Vazza CVF-2016-2021 X -/ genu-system.x85 CVF-2015-4224 Vestoria Vazza CVF-2016-2021 A.8 -/ X Opensitack Nova CVF-2015-5280 Vestoria Vazza Va	Ubuntu Update for (b)gas UN-295-1 Ubuntu Update for (b)gas UN-295-1 Ubuntu Update for (b)gas UN-216-1 Ubuntu Update for (b)gas UN-218-1 Bable (b)gas UN-218-1 Bable (b)gas UN-218-1 Bable (b)gas UN-218-1 (b)gas UN-218-1 (10.0 7.5 7.2 6.8 6.8	x x x	~ ~ ~ X	gemu-system-x86	CVE-2016-4008 CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Uburthu Update for test USH-2216-1 7.5 X ✓ Model CVE-2013-4522 CVE-2014-2381 Uburthu Update for test USH-216-1 7.2 X ✓ gemu-system-366 CVE-2013-4522 CVE-2014-2381 Uburthu Update for test USH-216-1 7.2 X ✓ gemu-system-366 CVE-2013-4544. CVE-2014-2381 Rester (define combo oilows to orefload more-compute 6.8 ✓ X OpenStack Nova CVE-2015-3280 Glance storage quote bypant when token is expliced 6.8 ✓ X OpenStack Nova CVE-2015-3280 Glance storage quote bypant when token is expliced 6.8 ✓ X OpenStack Keystone CVE-2015-5286 FK liben Revocation Bypast 6.0 ✓ X OpenStack Keystone CVE-2015-7346 Uburthu Update for FAM USN-235-2 5.8 X ✓ Ibpam-modules CVE-2015-7346 Uburthu Update for FAM USN-235-2 5.8 X ✓ Ibpam-modules CVE-2015-338. CVE- 2015-704 CVE-2015-338. CVE- 2015-704 CVE-2015-338. CVE- 2015-704 CVE-2015-338. CVE- 2015-704 CVE-2015-338. CVE- 2015-704	Usanta bydatic to source (24 124) Ubuntu Update for gett (24 24) 5-1 Ubuntu Update for gett (24 24) 5-1 Ubuntu Update for gett (24 24) 5-1 Resize/delete combo allows to overlaad nova-compute Nova may fail to delete images in resize table Glance storage quoto bypass when token is expired	7.5 7.2 6.8 6.8	x x v	×	gemu-system-x86	CVE-2013-7422, CVE-2016-2381 CVE-2013-4544, CVE-2014-2894
Libbulu bydał to reginu USI-122-1 7.2 X ✓ qemu-system-x86 CVE-2013-454.	Ubuntu Update for gemy USN-2182-1 Ubuntu Update for gemy USN-2182-1 Retize/delete combo allows to overload nova-compute Nova may fail to delete images in resize table Glance storage quoto byposs when token is expired	7.2 6.8 6.8	×	×	gemu-system-x86	CVE-2013-4544, CVE-2014-2894
Tubuntu Update for ABU UN-2182-11 7.2 X ✓ gemu-system x86 CVE-2013-4544. CVE-2013-4544. CVE-2013-42844. Restandelise combo allows to overhood nove compute 6.8 ✓ X Opentitack Nova CVE-2013-42844. CVE-2014-2894 Nova may fail to detele images in resize table 6.8 ✓ X Opentitack Nova CVE-2015-3280 Glance storage quoto bypars when token is expired 6.8 ✓ X Opentitack Nova CVE-2015-3286 Glance storage quoto bypars when token is expired 6.8 ✓ X Opentitack Revice CVE-2015-3286. Glance storage quoto bypars when token is expired 6.8 ✓ X Opentitack Revice CVE-2015-3286. Ubuntu Update for PAM UBX-235-2 5.8 X ✓ Ibpart-modules CVE-2015-3283. <	Ubuntu Update for gemy USN-2182-1 Resize/delete combo allows to averload nova-compute Nova may fail to delete images in resize table Glance storage quota bypass when token is expired	7.2 6.8 6.8	×	×	gemu-system-x86	CVE-2013-4544, CVE-2014-2894
Return / Control 6.8 ✓ X OpenStack Nova CVE-2015-3241 Nova moy fail of defile images in resize 6.8 ✓ X OpenStack Nova CVE-2015-3280 Nova moy fail of defile images in resize 6.8 ✓ X OpenStack Nova CVE-2015-3280 Glance storage audo bypcas 6.8 ✓ X OpenStack Nova CVE-2015-3280 Glance storage audo bypcas 6.8 ✓ X OpenStack Clance CVE-2015-3280 Glance storage audo bypcas 6.0 ✓ X OpenStack Clance CVE-2015-3286 Fill State Revocation Rypcas 6.0 ✓ X OpenStack Keytone CVE-2015-3286 CVE-2015-3286 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-3280 CVE-2015-3280 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-3280 CVE-2015-3280 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-3280 CVE-2015-3280 CVE-2015-3280	Resize/delete combo allows to overload nova-compute Nova may fail to delete images in resize fable Glance storage quota bypass when token is expired	6.8	1	x	Onesiteshile	
Fettler/clefete combo allow to overfload nov-compute 8.8 ✓ X OpenStack Nova CVE-2015-3241 Nove mys fait to detert images in resize tobio 6.8 ✓ X OpenStack Nova CVE-2015-3280 Glance storage quoto byposis when holen is expired 6.8 ✓ X OpenStack Nova CVE-2015-3280 Claince storage quoto byposis when holen is expired 6.8 ✓ X OpenStack Keystone CVE-2015-5286 Claince v2 AFL unrestricted path Averand Twoogh Riseystem 6.5 ✓ X OpenStack Keystone CVE-2015-7348 Ubuntu Update for PAM UBN-2935-2 5.8 X ✓ Ribpam-modules CVE-2015-7348 CVE-2015-7348 <td>Rest&/delete combo allows to overload nova-compute Nova may fail to delete images in resize table Glance storage quota bypass when token is expired</td> <td>6.8</td> <td>~</td> <td>x</td> <td>On an Physics Marco</td> <td></td>	Rest&/delete combo allows to overload nova-compute Nova may fail to delete images in resize table Glance storage quota bypass when token is expired	6.8	~	x	On an Physics Marco	
overland nova-compute Verland nova-compute Verland nova-compute Nova may fait bedret images in resize 6.8 ✓ X Opensitack Nova CVE-2015-3280 Glance strapped quota bypas 6.8 ✓ X Opensitack Nova CVE-2015-3280 Glance strapped quota bypas 6.8 ✓ X Opensitack Glance CVE-2015-3280 Glance strapped quota bypas 6.0 ✓ X Opensitack Keystone CVE-2015-7546 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-3238, CVE-2015-3238, CVE-2015-3238, CVE-2015-3238, CVE-2015-3238, CVE-2015-3239 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-3238, CVE-2015-3239 Togating header Kinage-meta-staturi S.5 ✓ X Opensitack Keystone CVE-2015-3231 Togating header Kinage-meta-staturi S.1 ✓ X Opensitack Keystone CVE-2015-3231 Liboaccitage S.1 ✓ X Opensitack Keystone CVE-2015-3232 Liboaccitage S.1 ✓ X	overload nova-compute Nova may fail to delete images in resize table Glance storage quota bypass when token is expired	6.8			Openstack Nova	CVE-2015-3241
Nov amplified deter images in resize 6.8 ✓ X OpenStack Nova CVE-2015-3280 Giance storage quote bypass 6.8 ✓ X CVE-2015-5286 Giance storage quote bypass 6.8 ✓ X CVE-2015-5286 Giance storage quote bypass 6.8 ✓ X OpenStack Keytone CVE-2015-5286 Giance v2 AFI unvesticited path swared Intrough Resystem 6.5 ✓ X OpenStack Keytone CVE-2015-7346 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-7346 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-338. CVE- 2015-7041. CVE-2014-2333. Ubuntu Update for PAM USN-2935-2 5.8 X ✓ Ibpam-modules CVE-2015-338. CVE- 2015-7041. CVE-2014-2333. Indep status can be changed by parating header kimage-methodiat 5.1 ✓ X OpenStack Nova CVE-2015-2599 INVa conside Costilian Meanstree via OUX conside Costilian Meanstree via OUX conside of table. 5.1 ✓ X OpenStack Keystone CVE-2015-3129 Vi	Nova may fail to delete images in resize table Glance storage quota bypass when token is expired	6.8		1		
Nova motor Check Status Construct Nova CVE-2015-288 Clance storage quote bypas 6.8 7 X Opensitack Nova CVE-2015-288 Glance V2 APT Unrestricted polh 6.5 7 X Opensitack Revision CVE-2015-288 Glance V2 APT Unrestricted polh 6.5 7 X Opensitack Revision CVE-2015-7546 Ubuntu Update For ANU USN-2935-2 5.8 X 7 Bipam-modules CVE-2015-7546 Ubuntu Update For ANU USN-2935-2 5.8 X 7 Bipam-modules CVE-2015-3288, CVE- 2015-7244 Ubuntu Update For ANU USN-2935-2 5.8 X 7 Bipam-modules CVE-2016-2833 Ubuntu Update For ANU USN-2935-2 5.8 X 7 X Opensitack Revision CVE-2016-2033 Toposing header Kwingge-meto-totack 5.5 7 X Opensitack Revision CVE-2015-2031 Nova conside Cross Bite Methods 5.1 7 X Opensitack Keystone CVE-2015-2037 States Incorrect concilian 4.3 7 X Opensitack K	table Glance storage quota bypass when token is expired	0.0		v	O	01/5 001/5 0000
Colline atorage quote bypois 4.8 / X CVE-2015-5284 Colline of ART unretricted path 6.5 / X OpenStack Glance CVE-2015-5284 Colline of ART unretricted path 6.5 / X OpenStack Glance CVE-2015-5284 Colline of ART Unretricted path 6.5 / X OpenStack Revisione CVE-2015-5284 Cuburbuil Update for PAM USN-2935-2 5.8 X / Ibpart-modules CVE-2015-2584. Uburbuil Update for PAM USN-2935-2 5.8 X / Ibpart-modules CVE-2015-2584. Uburbuil Update for PAM USN-2935-2 5.8 X / Ibpart-modules CVE-2015-2583. Uburbuil Update for PAM USN-2935-2 5.8 X / Ibpart-modules CVE-2015-2833. Uburbuil Update for PAM USN-2935-2 5.8 X / Repetition Non-2015 CVE-2014-2830. Indige trap cambel status 5.1 / X OpenStack Revice CVE-2015-2529 All Dramatic status 5.1 / X OpenStack Revice <	Glance storage quota bypass when token is expired		1	^	Openstack Nova	CVE-2015-3280
when token if expired Col X OpenStack Glance CVE2015-105 Glance V2 API unrestricted polh werned through flagviern 6.5 ✓ X OpenStack Glance CVE2015-1155 Glance V2 API unrestricted polh werned through flagviern 6.0 ✓ X OpenStack Keytone CVE2015-7546 Ubuntu Update For AMU USN-2935-2 5.8 X ✓ Bippam-modules CVE2015-3238, CVE- 2015/2011, CVE2014-2833 Ubuntu Update For AMU USN-2935-2 5.8 X ✓ Bippam-modules CVE2015-3238, CVE- 2015/2011, CVE2014-2833 Dispring header Kwage-meto-tothory 5.5 ✓ X OpenStack Glance CVE2015-2031 Now conclube Cors-Bite WebSocket 5.1 ✓ X OpenStack Nova CVE-2015-0239 All PUT Bracket Regl existence via OLO monified tock 5.1 ✓ X OpenStack Keytone CVE-2015-1852 Status Incorrect condition 4.3 ✓ X OpenStack Keytone CVE-2015-3182 Usuntu Update for cipic USN- 4.3 ✓ X OpenStack Cinder CVE-2015-1852 UBautus Updat	when token is expired	6.8	1	¥		CVE-2015-5284
Consect 24 Junesticited path Investig through filesystem 6.5 Y OpenStack Skince CVE-2015-1195 R1 kater, Revocition Byposs 6.0 Y X OpenStack Keystore CVE-2015-7346 Ubuntu Update for PAM USN-2935-2 5.8 X Y Ibpam-modules CVE-2015-7346 Ubuntu Update for PAM USN-2935-2 5.8 X Y Ibpam-modules CVE-2015-338, CVE- 2013-701, LVE-2014-2833 Ubuntu Update for PAM USN-2935-2 5.8 X Y Ibpam-modules CVE-2015-338, CVE- 2013-701, LVE-2014-2833 Image induct and be changed by passing header Kinage-mela-totatic 5.1 Y X OpenStack Clance CVE-2015-2037 1M Interdiction of the changed by passing header totatic 5.1 Y X OpenStack Nova CVE-2015-016 2.10 Provide totatic 5.1 Y X OpenStack Nova CVE-2015-016 3.1 For X OpenStack Keystone CVE-2015-016 CVE-2015-016 CVE-2015-016 3.1 For X OpenStack Keystone CVE-2015-014 CVE-2015-014 CVE-2015-014 2.1 Fordian Level on Administry	The second	0.0		~		010 1010 0100
Glance v2 API unretricited polt brownod through flexytem 6.5 ✓ X OpenStack Clance CVE2015-1195 PR Token Revocation bypos 6.0 ✓ X OpenStack Keytone CVE2015-7346 PR Token Revocation bypos 6.0 ✓ X OpenStack Keytone CVE2015-7346 Uburtu Update for PAM USN-2335-2 5.8 X ✓ Bibpam-modules CVE2015-7348, CVE- 2013-7041, CVE-2014-2383. Uburtu Update for PAM USN-2335-2 5.8 X ✓ Bibpam-modules CVE2015-7338, CVE- 2013-7041, CVE-2014-2383. Uburtu Update for PAM USN-2335-2 5.8 X ✓ X OpenStack Glance CVE2015-3238, CVE- 2013-7041, CVE-2014-2303. Uburtu Update for PAM USN-2335-2 5.1 ✓ X OpenStack Rova CVE2015-0239 All PUT Frazovick Eggl existence via OLO monified tock 5.1 ✓ X OpenStack Keytone CVE-2015-014 S3 Token Incorrect condition depression f033, Ipadated doctore 2.9 ✓ X OpenStack Keytone CVE-2015-1852 Uburtu Update for cpic UNN 2.9 ✓ X OpenStack Cinder						
Intervention through Resystem X OpenStack Keystone CVE-2015-7546 Ubunhu Update for PAM USN-2935-2 5.8 X ✓ Bipam-modules CVE-2015-7546 Ubunhu Update for PAM USN-2935-2 5.8 X ✓ Bipam-modules CVE-2015-7546 Ubunhu Update for PAM USN-2935-2 5.8 X ✓ Bipam-modules CVE-2015-2338, CVE- 2013-2701, CVE-2014-2333 Induct Update for PAM USN-2935-2 5.8 X ✓ Bipam-modules CVE-2015-2338, CVE- 2013-701, CVE-2014-2333 Induct Strange-meta-datu 5.1 ✓ X OpenStack Keystone CVE-2015-2037 Induct Strange-meta-datu 5.1 ✓ X OpenStack Keystone CVE-2015-0329 Induct Strange-meta-datu 5.1 ✓ X OpenStack Keystone CVE-2015-0314 Stoken Incore chandlion 5.1 ✓ X OpenStack Keystone CVE-2015-0329 Bip_Log Log Datameter of Reduk 5.1 ✓ X OpenStack Keystone CVE-2015-0329 Stoken Incore chandlion 5.1 ✓ X	Glance v2 API unrestricted path	6.5	1	x	OpenStack Glance	CVE-2015-1195
PK 10 ken Revocation Bypois 6.0 ✓ X OpenStack Keystone CVE-2015-7544 Uburnu Update for PAM UB-2335-2 5.8 X ✓ IBpam-modules CVE-2015-2308, CVE- 2015-2764, CVE-2012-2308, CVE- 2015-2764, CVE-2015-2014, CVE- 2015-2764, CVE-2015-2015, CVE- 2015-2764, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2017, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-2014, CVE-2015-201	traversal through filesystem					
Ubuntu Update for PAM USN-2935-2 5.8 X ✓ IBpam-modules CVE-2015-2036, CVE- 2013-2014, CVE-2014-2030 Ubuntu Update for PAM USN-2935-2 5.8 X ✓ IBpam-modules CVE-2015-2036, CVE- 2013-2014, CVE-2014-2030 Image atotus can be changed by parking header Kinage-meta-totus' 5.5 ✓ X OpenStack Kinage CVE-2014-2030 Nova concisie Cross- <u>Bite Metabockat</u> 5.1 ✓ X OpenStack Nova CVE-2014-2030 All PUT <u>Enstance</u> teal existence via Onterminited inductation 5.1 ✓ X OpenStack Nova CVE-2015-2037 All PUT <u>Enstance</u> teal existence via Onterminited inductation 4.3 ✓ X OpenStack Keytone CVE-2015-3219 Injection 4.3 ✓ X OpenStack Keytone CVE-2015-3219 Injection 4.3 ✓ X OpenStack Keytone CVE-2015-2037 Conder does not propenty track the life romat 4.0 ✓ X OpenStack Keytone CVE-2015-3219 Conder does not propenty track the life romat 4.0 ✓ X OpenStack Kindton CVE-2015	PKI Token Revocation Bypass	6.0	1	x	OpenStack Keystone	CVE-2015-7546
Uburhu Update for PAM UBN-2935-2 5.8 X ✓ Ibpammodules CVF-2015-2030; CVF-2015-2036; CVF-2015-2034; CVF-2015-2044; CVF-2015-2044; CVF-2015-2044; CVF-2015-2044; CVF-2015-						
Ubunhu Update for PAM USN-2935-2 5.8 X IBpammodules CVE-2011-CSR-2012-2883 CVE-2015-2012-CSR-2012-2883 Image atolus con be changed by passing heads Kinage-meta-stotaci 5.5 - X OpenStack Clause CVE-2015-2531 CVR-2012-2583 CVR-2012-2583 Japardin Locks Kinage-meta-stotaci 5.1 - X OpenStack Keystone CVE-2015-5259 All PUI Ensurés fagi existence via Do monified track-claison 5.1 - X OpenStack Keystone CVE-2015-0259 Big	Ubuntu Update for PAM USN-2935-2	5.8	x	1	libpam-modules	CVE-2015-3238, CVE-
Normoules CVE-2015-223.0. CVE-2015-203.0.					<i>n</i>	2013-7041, CVE-2014-2583
Image fatulus con be changed by posing head Y-kingge-mot-othory 5.5 / X Openstack Glance CVE2015203 Nova conside Cost Mite Medisockat, Nijociona 5.1 / X Openstack Kova CVE2015203 All PUT Branuk, Kagl withrone via OLO manifest otock 5.1 / X Openstack Keystone CVE20150239 All PUT Branuk, Kagl withrone via OLO manifest otock 5.1 / X Openstack Keystone CVE20150239 Status in Loomed cost 3.1 / X Openstack Keystone CVE20151852 Bib	UDUNTU Update for PAM USN-2935-2	5.8		~	libpam-modules	CVE-2015-3238, CVE-
Loading Insoder Verlage metal selection J. X Opensituek Solution CVE2015/02011 Nova cannable Consisting MetaSockat 5.1 X Opensituek Nova CVE2015/02011 Nova cannable Consisting MetaSockat 5.1 X Opensituek Nova CVE2015/02011 Nova cannable Consisting MetaSockat 5.1 X Opensituek Nova CVE2015/02011 Nova cannable Sockat 5.1 X Opensituek Nova CVE2015/02011 S0 Token Incore condition 4.3 X Opensituek Keystone CVE2015/82219 Molecular Doubletry Imm Vision Intervention 4.3 X Opensituek Noticon CVE2015/82037 20041 Ubuntu Update for cogo UBN- 4.3 X Cpensituek Noticon CVE2015/82037 20041 Tomat guessing and file reserve X Opensituek Cinder CVE2015/82037 20041 Tomat guessing and file reserve X Opensituek Honizon CVE2015/8204 2014 Z014 Z014 Z014 Z014 Z014 Z014/200 2014 <t< td=""><td>Image status can be observed by</td><td>6.6</td><td>1</td><td>×</td><td>OpenStack Clance</td><td>2013-7041, CVE-2014-2303</td></t<>	Image status can be observed by	6.6	1	×	OpenStack Clance	2013-7041, CVE-2014-2303
Journal of Lossing and Status 5.1 ✓ X OpenStack Nava CVE-2015-0259 All PUT Brayung Bag extenses via COL manifest analysis 5.1 ✓ X OpenStack Nava CVE-2015-0259 All PUT Brayung Bag extenses via COL manifest analysis 5.1 ✓ X OpenStack Keystone CVE-2015-014 S3 Token Incorrect condition 4.3 ✓ X OpenStack Keystone CVE-2015-014 Sa Token Incorrect condition 4.3 ✓ X OpenStack Keystone CVE-2015-0259 Winteroble to achitrary thmi 2.9 ✓ X OpenStack Keystone CVE-2015-2037 Value collable to achitrary thmi 2.9 ✓ X OpenStack Cinder CVE-2015-2037 Value collable to achitrary thmi 4.0 ✓ X OpenStack Cinder CVE-2015-2037 Tomad guesting and file formad guesting and file 4.0 ✓ X OpenStack Cinder CVE-2015-2015-2039 Another Horizon Logia ptoget 7.8 ✓ X OpenStack Ender CVE-2015-2019 Another Horizon Logia ptoget<	nassing header 'v image meta-status'	3.5	*	^	Opensidek Gidnee	040-2013-3231
Nova coulose Lossaitas un presponsational de la constructiona de la constenia de la constructiona de la constructiona de la const						
All FUll Engligits Big distinct on Via 5.1 / X OpenStack swift Cve-2015-014 OUX monited indick 3.1 / X OpenStack Keystone CVE-2015-1852 S3 Token Incorrect constition 4.3 / X OpenStack Keystone CVE-2015-1852 Sage Double for the field is 2.9 / X OpenStack Keystone CVE-2015-3152 High_Lists_Double for the field is 2.9 / X OpenStack Keystone CVE-2015-3129 High_Lists_Double for table for tab	Nova console Cross-site, Websocket	5.1	1	x	Openstack Nova	CVE-2015-0259
Not manifest attack I.I. X Openstack keytone CVE-2015-013 Stoken Locer condition 4.3 / X Openstack keytone CVE-2015-1832 Expl. togs convented of fields is their. togs convented of fields is bornhom. 2.9 / X Openstack Keytone CVE-2015-1832 Downhom Keytone CVE-2015-1832 CVE-2015-1832 CVE-2015-1832 CVE-2015-1832 Downhom Keytone A.3 / X Copenstack Keytone CVE-2015-1832 Conder does not properly track the file format 4.3 / X Copenstack Cinder CVE-2015-197, CVE-2015-2037 2399-1 4.3 / X Openstack Cinder CVE-2014-3341 Femal growing and tile disclosuring and containing 4.0 X Openstack Keystone CVE-2015-3844	All PUT tempurir leal existence via	6.1	1	×	OpenStack puift	Cum-2015-014
13 Token Incorrect condition 4.3 / X OpenStock KeyHone CVE-2015-1882 depression FS3, Indexing 4.3 / X OpenStock KeyHone CVE-2015-1882 depression FS3, Indexing 4.3 / X OpenStock KeyHone CVE-2015-1882 vibration for open fo	DIO manifest attack	5.1		^	opensidek swin	040-2013-010
expression for S3L Intercurve CVE-2015-3219 Vulnerable to arbitrary hmit light_total protection of fails is 2.9 / X OpenStack Horizon CVE-2015-3219 Vulnerable to arbitrary hmit light_total protection of the for gogle USN- 4.3 / X Calo CVE-2015-3219 V396-1 4.3 / X Calo CVE-2015-1197, CVE-2015-2037 CVE-2016-1197, CVE-2015-2037 Conder does not properly track the file format 4.0 / X OpenStack Cinder CVE-2016-43441 S31 horizon the totax regimes 7.8 / X OpenStack Cinder CVE-2015-3219 Vulnerability rotax 4.0 / X OpenStack Horizon CVE-2015-3219 Another Horizon login page vulnerability rotax 7.8 / X OpenStack Horizon CVE-2015-3219 Image dota memorini in backand dm back gogl 4.0 / X OpenStack Giance CVE-2015-3143 Image dota memorini in backand dm backand groupment containing 4.0 / X OpenStack Keystone CVE-2015-3446	\$3 Token incorrect condition	4.3	1	x	OpenStack Keystone	CVE-2015-1852
Hear parameter of fields is vulnerable to activitary html 2.9 X OpenStack Horizon CVE-2015-3219 Ubuntu Update for criging USN- 20661 4.3 ✓ X Cpio. CVE-2015-3219 Z0661 dates not properly track 4.0 ✓ X OpenStack Cinder CVE-2015-32037 Z0661 formation property track 4.0 ✓ X OpenStack Cinder CVE-2014-3240, CVE-2014-3641 Formatiopussing and file disclosure in Image convert reserve ✓ X OpenStack Cinder CVE-2015-3219 Another Instain login page Vulnerability to activitation 4.3 ✓ X OpenStack Horizon CVE-2015-3219 Another Instain login page Vulnerability to activitation 4.3 ✓ X OpenStack Horizon CVE-2015-3219 Another Instain login page Vulnerability to activitation 2.8 ✓ X OpenStack Horizon CVE-2015-3219 Image data semaline in backendi after deleting the image created using fack activity any model contactivity 4.0 ✓ X OpenStack Keystone CVE-2015-3446	expression for SSL insecure					
winercable to arbitrary hmi legication V X Cable CVE-2015-1197. CVE-2015-2037 Ubury Update for cypic USH- 4.3 / X Cable CVE-2015-1197. CVE-2015-2037 Cinder date not proceedly track 4.0 / X Openstrack Clinder CVE-2014-230. CVE-2014-3341 The file format Format guessing and file disclosure in image convert X Openstrack Clinder CVE-2015-3219 351 hortigan Hat dack reseline 4.3 / X Openstrack Hortizon CVE-2015-3219 Another Hortizon Digin page 7.8 / X Openstrack Hortizon CVE-2015-3219 Another Hortizon Digin page 7.8 / X Openstrack Hortizon CVE-2015-3143 Universitivity to a 20g_attack 8 / X Openstrack Glonce CVE-2015-3143 Image data memory in in backendi after developt fract memory controlling 4.0 / X Openstrack Keytone CVE-2015-3446	Help, text parameter of fields is	2.9	1	x	OpenStack Horizon	CVE-2015-3219
Injection CVE2015-1197. CVE2015-2037 Zhöel Uburtu Update for cpigu USN- Zhöel CVE2015-1197. CVE2015-2037 Zhöel CVE2014-220, CVE2014-220, CVE2014-3641 Format guesting and file reserve ✓ X OpenStack Cinder CVE2014-720, CVE2014-3641 Format guesting and file reserve ✓ X OpenStack Cinder CVE2015-1850 CVE2015-3129 XSS in Horizon Heat stack creation 4.3 ✓ X OpenStack Horizon CVE2015-3129 Another Horizon Lead stack creation 4.3 ✓ X OpenStack Horizon CVE2015-3143 Vuinerability to a Qbg attack Image data remains in backend offer deleting the mage created using 4.0 ✓ X OpenStack Glance CVE2015-3143 Vuinerability to a Qbg attack	vulnerable to arbitrary html					
Uburth Update for cigic USN- 4.3 / X Cable Core 2015-1187, CVE-2015-2037 Uburth Update for cigic USN- 4.0 / X OpenStack Cinder CVE-2015-1380, CVE-2015-2037 The file format Format guessing and file 4.0 / X OpenStack Cinder CVE-2015-1380 SS in Indian Heat Jock zeration 4.3 / X OpenStack Cinder CVE-2015-2397 Marchiter In Image convert 4.3 / X OpenStack Cinder CVE-2015-2397 Marchiter Indian Digin page 7.8 / X OpenStack Horizon CVE-2015-2319 Vulnerability To 2022 attrack 7.8 / X OpenStack Horizon CVE-2015-2319 Vulnerability To 2022 attrack 7.8 / X OpenStack Elevition CVE-2015-23143 Understand data remains in backend 4.0 / X OpenStack Clance CVE-2015-31881 Backend aurowers 5.0 X OpenStack Keystone CVE-2015-3464	injection					
20061 Index formal formal guesting and file 4.0 ✓ X OpenStack Cinder CVE-2014-7230, CVE-2014-3641 Formal guesting and file reserve ✓ X OpenStack Cinder CVE-2015-3150 Statist formal guesting and file reserve ✓ X OpenStack Cinder CVE-2015-3150 XS3 in Horizon Heat stack creation 4.3 ✓ X OpenStack Horizon CVE-2015-3219 Another Horizon login page 7.8 ✓ X OpenStack Horizon CVE-2015-3143 Uninecolity to a Dig affactor 8.0 ✓ X OpenStack Konizon CVE-2015-3143 Indire deleting the image created using there deleting the image created using task gait 4.0 ✓ X OpenStack Keystone CVE-2015-3143	Ubuntu Update for cpio USN-	4.3	1	x	Cplo.	CVE-2015-1197, CVE-2015-2037
Intellis formal CVE20147280, CVE20147881 CVE20147280, CVE20147881 CVE20147280, CVE20147881 CVE20147280, CVE20147881 CVE2014788 CVE20147280, CVE20147881 CVE2014788 CVE2014788 CVE2014788 CVE201478 CVE20148 CVE2014 CVE20148 CVE2014 CVE20148	2906-1	4.0		~	On an Stank Cinder	CIVE 0014 7020 CIVE 0014 2441
Terminal guesting and file reserve ✓ X OpenStack Cinder CVE-2015-1850 diclosure in Image convert 4.3 ✓ X OpenStack Cinder CVE-2015-3129 XSI horizon Heat stack creation 4.3 ✓ X OpenStack Horizon CVE-2015-3129 Another Horizon login page 7.8 ✓ X OpenStack Horizon CVE-2015-3143 Uninercolifity to a blog affaction 8.0 ✓ X OpenStack Horizon CVE-2015-5143 Image data remains in backend affar dening the image created using that dening the image created using task gall 0 ✓ X OpenStack Kaince CVE-2015-3143 Task gall Backend.argument controlling 4.0 ✓ X OpenStack Keystone CVE-2015-3546	the file format	4.0	ľ.	^	Opensidek Cinder	CVE-2014-7230, CVE-2014-3841
disclosure in image convert Factor / X Openstack strate OF 2215 State XS3 in Horizon Head fack reading 4.3 ✓ X Openstack Horizon CVE-2015-2019 Ancher Horizon kopin page vulnerability to a Dog attack 7.8 ✓ X Openstack Horizon CVE-2015-3143 Image data remains in backend after deleting the image cented using factered augument containing 4.0 ✓ X Openstack Keystone CVE-2015-3143	Format quessing and file	recenve	1	¥	OpenStack Cinder	CVE-2015-1850
Ass in hotion heat idock creation 4.3 ✓ X OpenStack Horizon CVE-2015-3219 Another traticin login page 7.8 ✓ X OpenStack Horizon CVE-2015-3219 Vuineroliiity to a 20g/attock X OpenStack Horizon CVE-2015-3143 Image data remains in backending there develop the image created using the develop the image created using task page X OpenStack Glance CVE-2015-31881 Task page Sackend-argument controlling 4.0 ✓ X OpenStack Keystone CVE-2015-3846	disclosure in image convert	1000110		^	oponoracie olinaci	012 2010 1000
XS3 in Notion Head tack reaction 4.3 / X OpenStack Horiton CVE-2015-3219 Ancher Horiton bigh page 7.8 / X OpenStack Horiton CVE-2015-3219 wuinerability to a <u>Dogs</u> attack // X OpenStack Horiton CVE-2015-3143 Image data remains in backend after deleting the mage created using tack adjug 4.0 / X OpenStack Glance CVE-2015-1881 Eackend, argument containing 4.0 / X OpenStack Keystone CVE-2015-3644						
Another trotton login page 7.8 / X OpenStack Hotton CVE-2015-5143 Image data remains in backend after delength in image readed using lask pgl 4.0 / X OpenStack Glance CVE-2015-51881 Eackend, argument controlling 4.0 / X OpenStack Keystone CVE-2015-5143	XSS in Horizon Heat stack creation	4.3	1	x	OpenStack Horizon	CVE-2015-3219
wuhresbillty to a Dog antock Image data remains in backend 4.0 ✓ X OpenStack Glance CVE-2015-1881 ander deleting the image created using task agai Backend, augument containing 4.0 ✓ X OpenStack Keystone CVE-2015-3846	Another Horizon login page	7.8	1	х	OpenStack Horizon	CVE-2015-5143
Image data menaini in backandi differ deleting fine mage created using bak togi <u>Scated, aryument</u> containing 4.0 X OpenStack Giance CVE-2015-1881 Scated, aryument control in the mage created using 4.0 X OpenStack Keystone CVE-2015-3846	vulnerability to a DoS attack					
Image data remains in backend 4.0 2 X Openstack cliance CVE-2015-1881 after deleting the image created using task ggl Backend, argument containing 4.0 2 X OpenStack Keystone CVE-2015-3646		-				
arter deterning me introdie created using Tarkit gpl Backend_argument containing 4.0 ✓ X OpenStack Keystone CVE-2015-3646	Image data remains in backend	4.0	1	x	OpenStack Glance	CVE-2015-1881
Backend_graument containing 4.0 ✓ X OpenStack Keystone CVE-2015-3646	tark ani					
and a second a s	Backend, argument containing	4.0	1	¥	OpenStack Keystone	CVE-2015-3646
password leaked in loas	password leaked in loas	1.0		^	oponologic koyalono	012 2010 0010
Adding 0.0.0.0/0 glowed 4.0 X OpenStack Neutron CVE-2015-3221	Adding 0.0.0.0/0 allowed	4.0	1	x	OpenStack Neutron	CVE-2015-3221
address pairs breaks L2 agent	address pairs breaks L2 agent					
Image data stays in store if 4.0 🗸 X OpenStack Glance CVE-2015-3289	Image data stays in store if	4.0	~	x	OpenStack Glance	CVE-2015-3289
image is deleted after creating	image is deleted after creating					
image using import task	image using import task	-				
Format-guessing and file 3.5 - X OpenStack Glance CVE-2015-5163	Format-guessing and file	3.5	1	х	OpenStack Glance	CVE-2015-5163
Lasciosure via image conversion	assciosure via image conversion	26		v	One shark black	CV/E 0014 4040
	canbe byparred by changing	3.5	ľ		Opensidck-Neutron	CVE-2013-5240
IP, MAC and DHCP spoofing rules a.5 X OpenStack-Neutron CVE-2015-5240 CVE-2015-5240	device owner				1	

Figure 3: Comparison table showing vulnerabilities discovered by CAVAS and OpenVAS.

mis-configurations in the deployed targets using information obtained from OSSN. We then conduct credentialed scans against the target cloud using CAVAS. We repeat the same experiments against "vanilla" OpenVAS and the community edition of Nessus scanner. As shown in Figure 3, the number of vulnerabilities discovered via our approach out-numbers those identified with OpenVAS. While CAVAS identifies 23 vulnerabilities, OpenVAS identifies 9 vulnerabilities. Note also that the vulnerabilities identified by OpenVAS are not specific to OpenStack, they are generic Linux vulnerabilities affecting third-party applications e.g. OpenSSL. We do not include the results of Nessus since the scanner only identified host and enumerated running services without identifying vulnerabilities.

We note however that most of the vulnerabilities discovered via with "vanilla" OpenVAS have higher CVSS scores. We also observe that the other vulnerability scanners do not have security policies for scanning OpenStack resources such as configuration files and Database-as-a-Service (DBaaS). Also, security best practices are not implemented in these scanners as done in CAVAS. We observed that several vulnerabilities do not have appropriate plugins in OpenVAS, for example CVE-2015-3241 (Figure.2), but CAVAS identifies this vulnerability (Listing 1) since we implemented appropriate plugin. Our approach is therefore suitable for deployment in a VAaaS where customers with minimum security expertise can employ it in securing their cloud environments.



Listing 1: Result of Plugin Identifying CVE-2015-3241 Vulnerability.

VII. FUTURE WORK

We have applied our framework from the perspective of a cloud administrator. It could be interesting to consider the cloud customer use case. We envisage that in such a scenario, other factors such as scalability and elasticity of the VAaaS would be an important factor, as well as the dynamic nature of cloud instances and resources. Similarly, it is important to extend our approach to include advanced web application scanning capabilities such as fuzzing. This is a useful requirement considering that cloud services are generally accessed through the web interface. Also, integration of other OpenStack services such as swift for storing scanning data such tasks, reports and targets is interesting. Similarly, a useful feature could be integration of threat intelligence frameworks for fast and effective sharing of vulnerability information across OpenStack cloud deployments. This feature has been recommended by CSA [29] and relevant frameworks can be utilized e.g. Security Content Automation Protocol (SCAP), Trusted Automated Exchange of Indicator Information (TAXII) and Cyber Observable Expression (CybOX). Security monitoring and information analytics is useful component for secure environments. OpenStack Telemetry is a project aimed at reliably collecting information on the utilization of physical and virtual resources in an OpenStack cloud. The project is geared towards offering MONaaS in OpenStack. It consists of OpenStack services e.g. Ceilometer, Aodh and Gnochi. An investigation into effective approaches for deploying VAaaS alongside MONaaS is an open research question.

VIII. CONCLUSION

OpenStack is a popular open-source IaaS cloud computing framework that offers almost every cloud package available on AWS as well as other major CSPs. It is officially supported by over 100 companies however there are few productionready deployments. This low deployment trend is attributed to security issues, amongst other factors. Several commendable efforts have been made to improve security in recent OpenStack releases. But, these efforts are more beneficial to developers than cloud administrators and normal users. However, a core characteristic of the cloud is self service. One of the major security requirements for cloud services is vulnerability assessment which are essential aspects of any audit and regulatory compliance requirements. Such a service is not available in OpenStack. Accordingly, in this work we have implemented CAVAS, a prototype that provides first steps to integration of VAaaS in OpenStack. We focus on identifying vulnerabilities that are specific to OpenStack core services and software and not those affecting other third party software. We leverage on information provided from public vulnerability information resources such as NVD and OSVDB. Our approach differs from existing solutions in that we also include information published by the OpenStack Security group; OSSA and OSSN. Accordingly, we are able to automate vulnerability assessment and dramatically improve scanning accuracy. We envisage that our approach could be useful for security assessments of OpenStack including vulnerability assessments and security auditing for regulatory compliance.

REFERENCES

- RightScale, "State of the cloud report", *State of the Cloud Report*, 2016. [Online]. Available: http://www.rightscale.com/lp/2016-state-of-the-cloud-report? campaign=701700000015euW.
- [2] OpenStack Foundation, Openstack cloud software. [Online]. Available: http://www.openstack.org/.
- [3] VMWare. [Online]. Available: https://www.vmware. com/cloud-computing/private-cloud.
- [4] Talligent, State of openstack adoption report industry survey results 2016, Report, 2016.
- [5] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

- [6] CSA, Secaas implementation guidance category 10 network security, Cloud Security Alliance, 2012.
- [7] Kennedy A Torkura, Feng Cheng, and Christoph Meinel, "A proposed framework for proactive vulnerability assessments in cloud deployments", in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2015, pp. 51–57.
- [8] Burton S Kaliski Jr and Wayne Pauley, "Toward risk assessment as a service in cloud environments.", in *HotCloud*, 2010.
- [9] Sasko Ristov, Marjan Gusev, and Aleksandar Donevski, "Openstack cloud security vulnerabilities from inside and outside", *CLOUD COMPUTING*, pp. 101–107, 2013.
- [10] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "Vulcan: Vulnerability assessment framework for cloud computing", in *Software Security* and Reliability (SERE), 2013 IEEE 7th International Conference on, Jun. 2013, pp. 218–226. DOI: http://dx. doi.org/10.1109/SERE.2013.3110.1109/SERE.2013.31.
- [11] Patrick Kamongi, Mahadevan Gomathisankaran, and Krishna Kavi, "Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing", 2015.
- [12] Richard Li, Dallin Abendroth, Xing Lin, Yuankai Guo, Hyun-Wook Baek, Eric Eide, Robert Ricci, and Jacobus Van der Merwe, "Potassium: Penetration testing as a service", in *Proceedings of the Sixth ACM Symposium* on Cloud Computing, ACM, 2015, pp. 30–42.
- [13] Mohamed Almorsy, John Grundy, and Amani S Ibrahim, "Vam-aas: Online cloud services security vulnerability analysis and mitigation-as-a-service", in *Web Information Systems Engineering-WISE 2012*, Springer, 2012, pp. 411–425.
- Bernd Grobauer, Tobias Walloschek, and Elmar Stocker, "Understanding cloud computing vulnerabilities", *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50–57, 2011, ISSN: 1540-7993. DOI: http://dx.doi.org/http://doi. ieeecomputersociety.org/10.1109/MSP.2010.115http: //doi.ieeecomputersociety.org/10.1109/MSP.2010.115.
- [15] Openstack Foundation. (Aug. 15, 2016). Openstack cloud software. OpenStack Cloud Software, [Online]. Available: http://www.openstack.org/ (visited on 08/16/2016).
- [16] OpenStack, Openstack security, Online, Openstack Security. [Online]. Available: https://wiki.openstack.org/ wiki/Security.
- [17] OpenStack Foundation, Vulnerability management process, online. DOI: http://dx.doi.org/10.1016/s1874-5970(05)80009-810.1016/s1874-5970(05)80009-8.
 [Online]. Available: https://security.openstack.org/vmt-process.html.
- [18] Openstack Foundation, *Openstack monitoring*. [Online]. Available: https://wiki.openstack.org/wiki/MONaaS.
- [19] OpenStack Foundation, *Openstack releases*, Online. [Online]. Available: http://releases.openstack.org/.

- [20] Dave Shackleford, "Virtualization and cloud: Orchestration, automation, and security gaps", [Online]. Available: https://www.rsaconference.com/writable/ presentations/file_upload/csv-r02-virtualization-andcloud-orchestration-automation-and-security_gaps_v2. pdf.
- [21] Mohamed Almorsy, John Grundy, Ingo Müller, et al., "An analysis of the cloud computing security problem", in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov, 2010.
- [22] Amazon inspector user guide. [Online]. Available: http: //docs.aws.amazon.com/inspector/latest/userguide/ inspector-ug.pdf.
- [23] "Amazon web services: Overview of security processes", Amazon Whitepaper, Nov. 2014. [Online]. Available: https://media.amazonwebservices.com/pdf/ AWS_Security_Whitepaper.pdf.
- [24] Eric Whyne Seymour Bosworth Michel E. Kabay, Computer Security Handbook, Sixth. John Wiley & Sons, 2014.
- [25] OpenStack, OpenStack Security Guide, OpenStack, Ed. OpenStack Foundation, 2016.
- [26] A. Nakamura, "Towards unified vulnerability assessment with open data", in *Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual*, Jul. 2013, pp. 248–253. DOI: http: //dx.doi.org/10.1109/COMPSACW.2013.3410.1109/ COMPSACW.2013.34.
- [27] Kennedy A Torkura, Feng Cheng, and Christoph Meinel, "Application of quantitative security metrics in cloud computing", in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2015, pp. 256–262.
- [28] Weidong Cui, M. Peinado, H.J. Wang, and M.E. Locasto, "Shieldgen: Automatic data patch generation for unknown vulnerabilities with informed probing", in *Security and Privacy*, 2007. SP '07. IEEE Symposium on, May 2007, pp. 252–266. DOI: http://dx.doi.org/10. 1109/SP.2007.3410.1109/SP.2007.34.
- [29] CSA, Secaas implementation guidance category 5 : Security assessments, Cloud Security Alliance, 2012. [Online]. Available: https : / / downloads . cloudsecurityalliance . org / initiatives / secaas / SecaaS_Cat_5_Security_Assessments_ Implementation_Guidance.pdf.