ORACLE

Oracle Cloud Infrastructure Vulnerability Scanning Service

Cloud Security Instance Scanning for Oracle Cloud Infrastructure

Technical Brief
June 2021, Version 1.5

Public

Purpose statement

This document provides an overview of features and enhancements included in Oracle Cloud Infrastructure—OCI. It is intended solely to help inform decision making around I.T. projects.

Intended Audience

Any OCI user that requires OCI Compute instance monitoring and alerting to identify ports left unintentionally open, installed packages that contain known vulnerabilities, and insecure configurations by collecting Center for Internet Security (CIS) Benchmark results.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Introduction

Vulnerabilities are weaknesses that when successfully exploited can provide an attacker the ability to gain access and take control of resources. Customers need tools and processes to help them identify and prevent common vulnerabilities to protect their resources against attacks. For example, organizations must take measures to secure the configuration of unused ports, software packages, container images, and instances and then update those configurations regularly to prevent vulnerabilities. Vulnerability scanning is a common compliance requirement (e.g., NIST 800-53 Rev.4 FISMA) for customers and a recommended security best practice for all organizations. Customers face challenges with scanning due to:

1. Disjointed vulnerability scanning tools—Often, customers will buy or license multiple tools for scanning instances, containers, and applications. The total cost can add up, leaving customers to choose between cost and security.
2. Lots of manual processes to correct vulnerabilities—Customers must deploy, configure, and upgrade agents on their fleets, with large operational pain, and the potential for misconfiguration due to human error.
3. Large volume of alerts with a high false positive rate—Vulnerability reports can overwhelm customers with "noise". Too many false positive findings will cause customers to get lost in the volume or get accustomed to it. As a result, this can reduce the time to resolution for critical issues or even worse, these critical issues can go unacknowledged.

Executive Summary

Oracle Cloud Infrastructure Vulnerability Scanning Service (OCI VSS) is simple, prescriptive, and tightly integrated with the OCI platform. VSS is available to all OCI customers that have paid accounts at no additional cost. The scanning platform includes default plugins and engines for instance and container scanning. The service scans installed packages and artifacts looking for the existence of known vulnerabilities. The service scans for open ports on an instance and it reports on publicly and privately available open ports. These findings will highlight what ports an attacker might use or what application could be shut down by the customer to reduce their attack surface. The scanning agent also reviews the configuration of each instance against specific OS CIS benchmarks enabling customers to see immediately what Operating System (OS) security hardening opportunities exist on their instances.

VSS manages the deployment, configuration, and upgrade of these engines and agents across the customer's OCI tenancy fleet. VSS reports all the findings as problems through Oracle Cloud Guard, with rules and machine learning to prioritize vulnerabilities. Cloud Guard alerting can help customers reduce the time from detection to remediation.

The OCI Vulnerability Scanning Service enables customers to target scans against their instances in a compartment, sub-compartments, or for specific instances. For each target, a user can configure the service to:

- Scan all their compute instances created from any of the OCI Compute base images: Oracle Linux, CentOS, Ubuntu, or Windows Server. Any custom image that is created from one of these base operating systems can also be scanned by our plugin.

- The VSS plugin:
    - Looks for installed packages with known vulnerabilities identified by Common Vulnerabilities and Exposures (CVEs) identifiers listed in the National Vulnerability Database—NVD.
    - Looks for configurations that meet or miss specific OS Linux CIS Benchmarks for authorization and access. In the future, VSS will add full OS CIS benchmarks for the base OCI Compute images that were listed above.
    - Records what ports are open on the instance.
- Perform a network scan of all public facing IPs on the targeted instances. This show which ports are reachable with the current networking rules in use.
- Scan Oracle Cloud Infrastructure Container Registry (OCIR) container images for installed packages that contain known vulnerabilities. This feature is available through OCIR, and it provides visibility into container image vulnerabilities on a regular cadence as new vulnerabilities are added to the database.

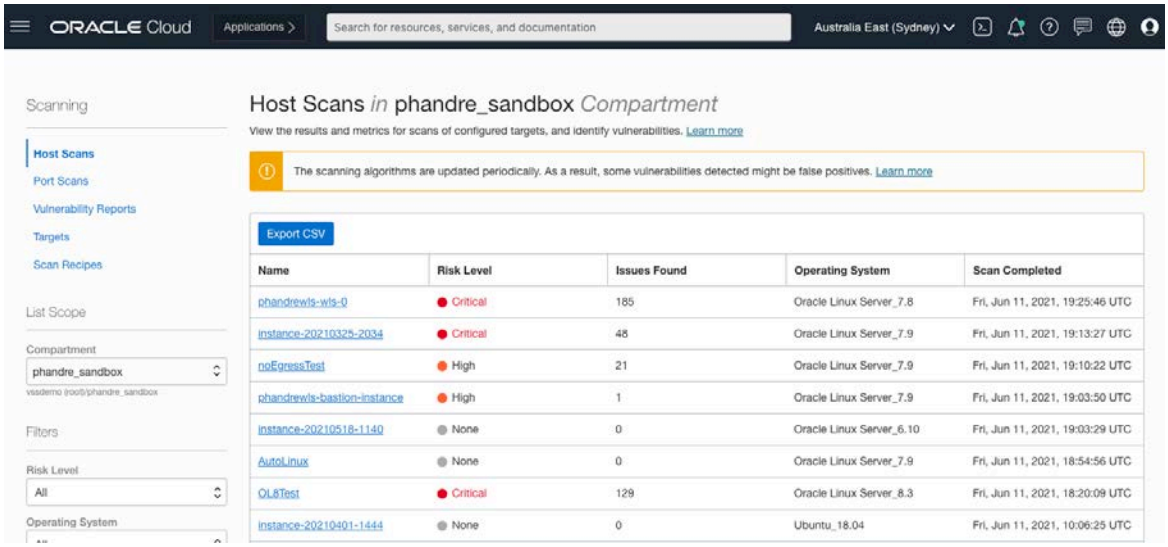
Cloud Guard enables users to configure the severity threshold— using the common vulnerability scoring system (CVSS) Base Score—used to determine which CVEs should be reported as problems for the instances scanned. In addition, Cloud Guard enables users to define what ports should not be open. This allows Cloud Guard to report non-allowed ports as a problem. Users can view all findings in the global reporting region of Cloud Guard so that they can monitor these security risks across all regions and assign the priorities of remediation.

Results

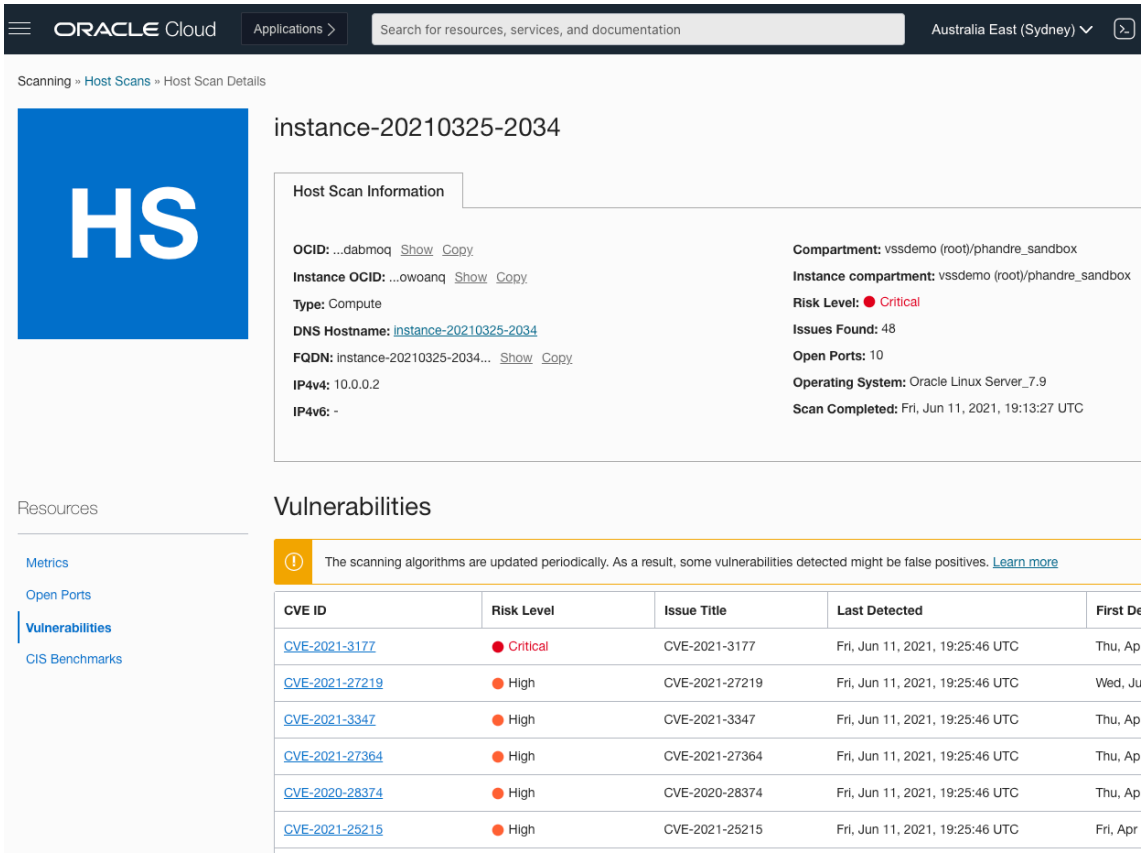
Once the instances have been scanned, the customer can sort and filter to find the instances impacted the most. The service gathers the latest CVEs from the open-source feeds from the National Vulnerability Database (NVD), RedHat and Oracle Linux and other Linux's OVAL feeds. This data is matched against the installed packages on the customer's compute instances. Matches are reported with the security risk and links to the National Vulnerability Database (NVD) about the details of what patches are needed to correct the vulnerability. Currently, VSS provides the details from NVD as the remediation next step. In the future Cloud Guard will add remediation actions for customers to address problems identified as vulnerabilities.

The Common Vulnerability Scoring Systems v3.0 (CVSS) Base Score of each matched CVE gets mapped to severity levels (critical, high, medium, low, and none) and these severity levels map to the risk levels used by Cloud Guard. On these report listing pages, the highest risk level found on an instance and the number of issues found will be shown. The list will always default to the items most recently scanned. All findings flow to the event and logging streams and can be then used by other systems like a SIEM.

A typical list of hosts that have been scanned:



Detail Host scan results with the vulnerabilities listed:



Conclusion

With Oracle VSS, customers can quickly and automatically identify possible vulnerabilities and common configuration mistakes thus improving the security postures of their OCI instances. After a customer creates a scan target against a compartment then they know that all current and future instances created in that compartment or sub-compartments will get scanned and a report will be created. Oracle Cloud Infrastructure Vulnerability Scanning Service is simple to turn on, and the agent is installed and updated automatically. Customers can use the service to scan OCI Compute instances with no additional costs. The service helps reduce the overall operational burden with managing agents and onboarding new instances. The detectors in Cloud Guard can be fine-tuned by adjusting the non-allowed ports and alert levels so that the correct level of problems gets alerted for administrators to see.

Further Reading

To learn more about OCI scanning and vulnerabilities, Cloud Guard, or deeper knowledge on OCI see the following resources:

- How to use the Vulnerability Scanning Service
- Getting Started with Cloud Guard
- National Vulnerability Database