ORACLE

Secure Oracle JD Edwards Deployments on Oracle Cloud Infrastructure with Oracle Vulnerability Scanning Service

Configurations and Best Practices for Setting Up Oracle Vulnerability Scanning Service with Oracle JD Edwards EnterpriseOne on Oracle Cloud Infrastructure

November, 2021, Version 2.1

Purpose statement

This document describes how to keep Oracle JD Edwards deployments on Oracle Cloud Infrastructure secure with Oracle Vulnerability Scanning Service, how to fix the issues found during the scan, and the best practices to keep instances secured.

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.

Table of contents

List of images

Introduction

Security is of paramount importance to Oracle JD Edwards customers in their digital transformation journey. It is important for our customers to consider security at every aspect of their digital transformation, cloud being one of them. Customers using Oracle JD Edwards on Oracle Cloud Infrastructure customize their architectural layout and integrations based on their business requirements. These architectural changes such as external integrations, port changes, VCN configurations, and so on may introduce security vulnerabilities to their Oracle JD Edwards instance if they have not followed adequate security measures. These vulnerabilities might increase the risk drastically to customers if they are not identified and fixed over a long period of time. Customers currently do not have the right tools to perform security scans on their Oracle JD Edwards on Oracle Cloud Infrastructure and fix any vulnerabilities.

The Oracle Cloud Infrastructure Vulnerability Scanning Service (VSS) provides a simple, on by default, prescriptive, and free scanning suite that is tightly integrated with the Oracle Cloud Infrastructure platform. Oracle VSS helps improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. This capability provides a significantly more proactive approach for Oracle JD Edwards customers to keep their deployments secure on Oracle Cloud Infrastructure. The scanning service provides default plugins based on open-source scanning engines for host and container image scanning. This service manages the deployment, configuration, and upgrade of these engines and agents across the customer fleet. All problems detected by the scanning service are presented in Oracle Cloud Guard, with rules and ML to prioritize critical vulnerabilities. Subsequently, Oracle Cloud Infrastructure takes action (alert, auto-remediate, or quarantine) using responders to shorten the response time from detection to remediation.

With Oracle VSS, Oracle JD Edwards customers can easily identify any old packages that are running on their hosts that could potentially be exploited by an attacker or if a default password is being used on an open port that was not supposed to be actively running. Oracle JD Edwards customers may also neglect the hardening of hosts after they get past the initial deployment. Oracle VSS helps customers identify these problems early and aids in remediation. More details are available at https://docs.oracle.com/en-us/iaas/scanning/using/overview.htm

Key Concepts

This document discusses the following key concepts and usage information about Oracle Vulnerability Scanning Service for Oracle JD Edwards customers:

Scan Recipe

This function defines scanning parameters for a type of cloud resource, including what information to examine and how often.

For more details, visit https://docs.oracle.com/en-us/iaas/scanning/using/managing-host-recipes.htm

Target

This can be one or more cloud resources that you want to scan using a specific scan recipe. Resources in a target are of the same type, such as compute instances.

For more details, visit https://docs.oracle.com/en-us/iaas/scanning/using/managing-host-targets.htm

Host Scan

This scan type provides metrics about a specific cloud resource that was scanned, including the vulnerabilities that were found, their risk levels, and CIS benchmark compliance.

The scanning service uses a host agent to detect these vulnerabilities.

For more details, visit https://docs.oracle.com/en-us/iaas/scanning/using/host-scan-reports.htm

Port Scan

This scan type lists the open ports that were detected on a specific cloud resource that was scanned.

To detect open ports, this scan uses a host agent or a network mapper that searches your public IP addresses.

For more details, visit https://docs.oracle.com/en-us/iaas/scanning/using/port-scan.htm

Vulnerability Report

This report provides information about a specific type of vulnerability that was detected in one or more targets, for example, a missing update for an OS package.

For more details, visit https://docs.oracle.com/en-us/iaas/scanning/using/host-vulnerabilities-reports.htm

Setup

To set up and use Oracle VSS, follow these steps:

1. Provide the required permissions to the service so that the plugin can run on every host and gather vulnerabilities, open port information, and CIS benchmark findings.
2. Create a scan recipe that describes the actions you want the host scanning service to perform.
3. Create one or more scan targets that use the recipe and the target compartments or instances to be scanned. If you point your scan target to root and all subcompartments, then all current and newly created instances are scanned.

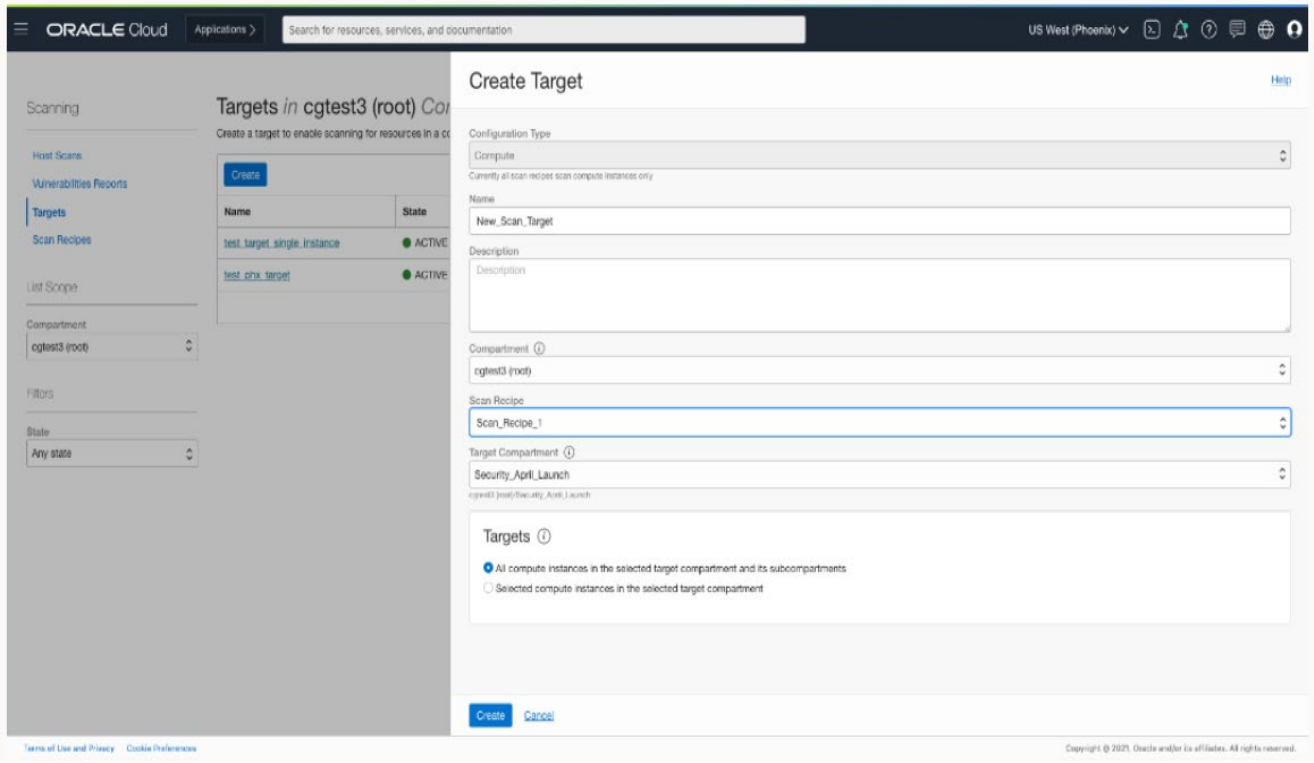

Image Caption 1. Create Target

Vulnerability Report

Security administrators can monitor the security posture of every host by viewing the vulnerability reports in the scans of your configured targets. A sample report is provided below.

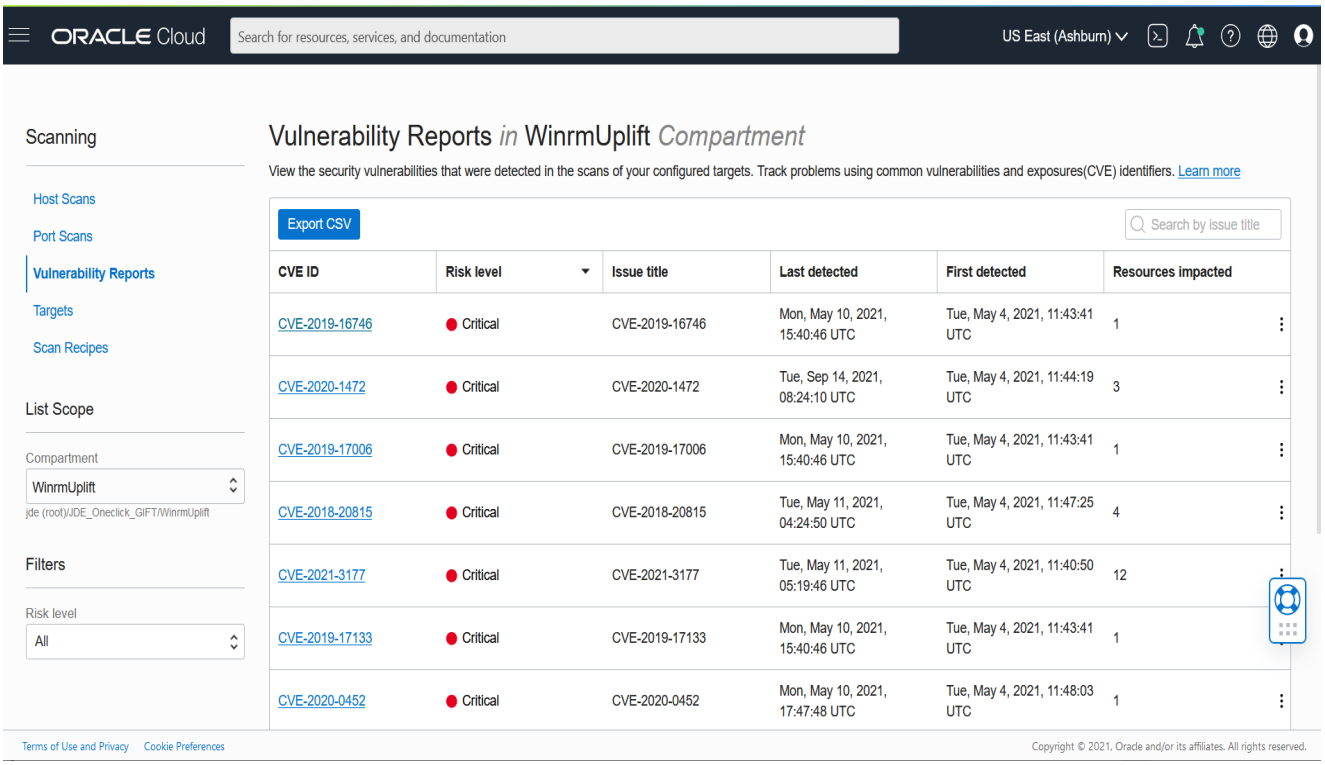

Image Caption 2. Vulnerability Report

You can find more details about the detected security vulnerabilities by clicking CVE-ID.

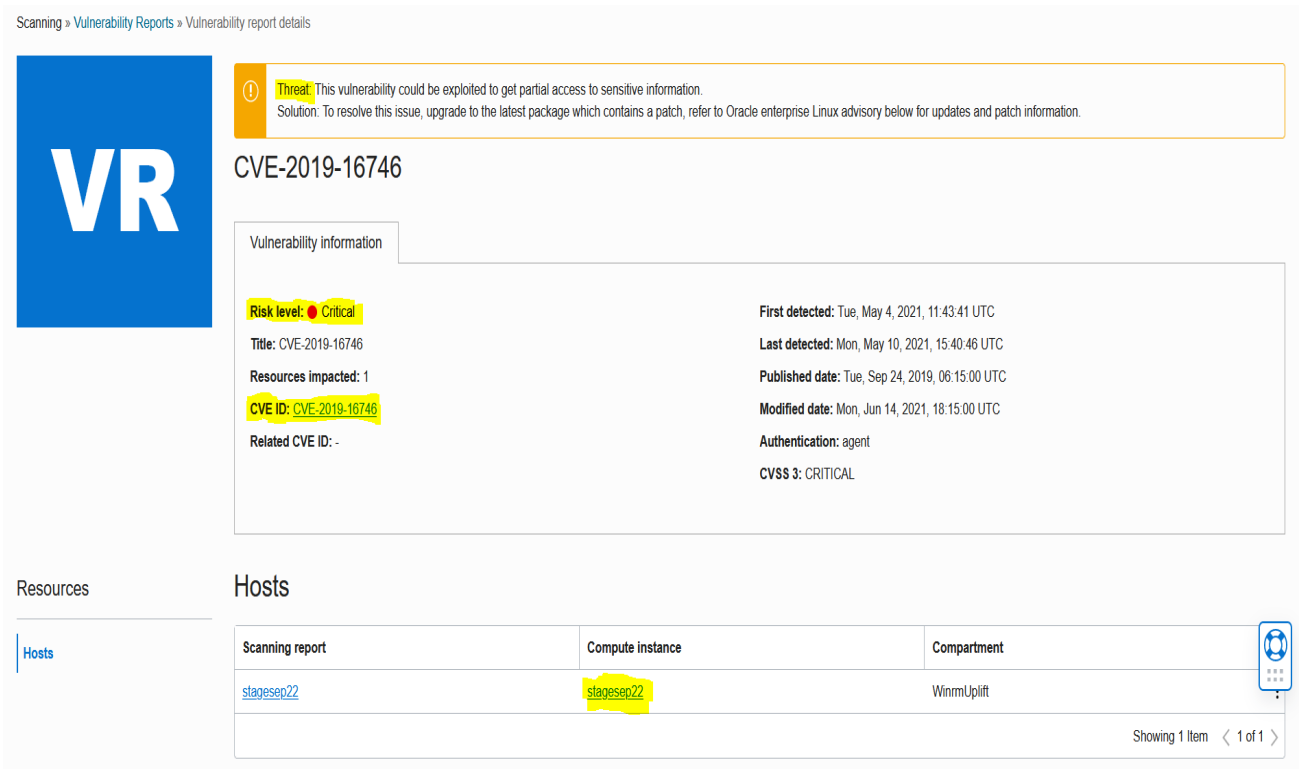

Image Caption 3. Vulnerability Information

On this screen, you can find a brief description of the CVE, the CVE risk level, detailed information and probable fix of the CVE, and compute instances impacted by CVE.

To fix issues with a CVE, follow the below steps.

1. Identify the vulnerable third-party package by searching for the CVE number on national vulnerability databases available publicly.
2. Identify the fix version or patch available.
3. Log in to your impacted compute instance and update the package or apply the fix patch.

Best Practices

The best practices to keep instances secured are as follows:

1. Open only those ports in security list and network security groups that are essential for an application, such as Oracle JD Edwards EnterpriseOne.
2. Provision all servers in private subnets and access them through bastion host.
3. Do not open any port to internet. Specifically admin application ports like DB EM console, WLS console or SM console. Limit port access to VCN CIDR if access is outside of VCN. You can control this with appropriate settings in the VCN CIDR for security lists and network security groups. Refer to these links:

   https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm

   https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm
4. If your application requires certain ports to be opened to the Internet, you should only open them for whitelisted IP addresses.
5. Keep the firewall on and only open the essential ports required for the application.
6. Use SSL-enabled web server ports only.
7. Use CA signed certificate instead of self-signed certificate for all servers running on HTTPS.
8. Use JDENET over SSL.
9. Use SQLNET (using Oracle Wallet) over SSL for DB connection from web server and enterprise server and deployment server.
10. Keep all components up to date with the latest available security patches.
11. Keep your SSH keys protected.
12. Use storage/disk encryption for all JDE E1 server compute storage and object storage. i. Use OCI vault to manage keys for encryption.
13. Use a strong password for your Microsoft Windows devices.
14. Configure Oracle VSS for your instances. For issues reported in a VSS scan report, identify the exact vulnerable component using the CVE and install the patch or update the component to the latest available version. Block or restrict any unnecessary port that is reported as open in the port scan report.
15. Plan a regular cadence of reviewing the vulnerability scan reports and taking necessary actions on a periodic basis to prevent any vulnerabilities.

Conclusion

Oracle VSS offers cloud-native vulnerability detection that provides Oracle JD Edwards customers and security administrators with a comprehensive view into potentially misconfigured or vulnerable hosts, making it simpler to detect and respond to any security vulnerabilities. Oracle JD Edwards customers can have a significantly more secure deployment on Oracle Cloud Infrastructure by leveraging the capabilities of Oracle VSS.

Oracle JD Edwards customers can leverage Oracle VSS for their Oracle JD Edwards instances on Oracle Cloud Infrastructure to identify and fix any security vulnerabilities. This helps customers in faster identification and resolution of security issues that might have been introduced due to architectural customizations and integrations. Customers can use this service to perform security scans on a periodic basis to take action on any new security

issues introduced by recent changes. This helps customers to create and maintain a highly secure and stable Oracle JD Edwards environment on Oracle Cloud Infrastructure.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle