White Paper: **September 2023**

Security Measures in VMware Application Catalog

Best practices to ensure open source software supply chain security

vmware®

Table of contents

About this white paper

This paper presents an overview of security measures implemented in VMware Application Catalog.

Risks of running open source in production

Open source software (OSS) has seen widespread adoption in recent years. In a recent technology research paper, expert analysts from the International Data Corporation (IDC)—Al Gillen, group vice president, software development and open source; Jim Mercer, research vice president, DevOps and DevSecOps solutions; and Katie Norton, senior research analyst, DevOps and DevSecOps —said that open source software is no longer a fringe technology used by leading-edge risk takers; rather, it has become a mainstream technology used to build applications, and its use will only increase in the future.[1] The State of Software Supply Chain: Open Source Edition 2022 said that open source technology has managed to fulfill its promise by delivering expected benefits, such as cost efficiency, increased flexibility and developer productivity. But a survey conducted as part of the same report showed that 94 percent of respondents have concerns about using OSS in production.[2] Of the 1,703 codebases audited as part of the 2023 Open Source Security and Risk Analysis report by Synopsys, 96 percent contained OSS components, while 84 percent had at least one open source vulnerability. More importantly, 48 percent of the examined codebases had high-risk vulnerabilities.[3]

To successfully secure an OSS supply chain, it is critical to gain visibility into the dependencies that OSS brings along, know about vulnerabilities in those dependencies, and have them patched as soon as possible. But keeping up to date on every OSS component and all its dependencies, vulnerabilities and patches in the upstream source code is a tedious and time-consuming effort that very few organizations can afford. The bigger question is whether development teams should be spending their time packaging OSS applications; manually tracking every single one of them and their dependencies; and ensuring they are all always up to date, healthy and patched with the latest CVE fixes rather than focusing on innovation and building new business solutions.

How VMware Application Catalog helps

VMware Application Catalog aims to enable enterprise developer teams to leverage the benefits offered by the OSS ecosystem while empowering platform engineering teams with optimal control and deep visibility into their OSS supply chains.

1. IDC, sponsored by VMware. “Ensure Secure Open Source Software Using Automated Tooling.” Al Gillen, Jim Mercer, Katie Norton. April 2023.
2. VMware. “The State of the Software Supply Chain: Open Source Edition 2022.” October 2022.
3. Synopsys. “2023 Open Source Security and Risk Analysis Report.” April 2023.

VMware Application Catalog is the enterprise version of the open source Bitnami Application Catalog. VMware Application Catalog is a library of more than 130 widely used OSS application components that are built to spec on top of base operating system (OS) images of a customer's choice. The images are continuously tested on various deployment platforms and are build-time scanned for vulnerabilities, helping make OSS more secure and production-ready. All images available in VMware Application Catalog are continuously maintained through an automated build pipeline, which tracks upstream OSS projects for any new upgrades, triggering an update/new build process and ensuring all images in the catalog are always up to date and secure. Before delivering images to the private registry of a customer's choice, the build pipeline securely packages the images, then tests them for functionality on multiple cloud and Kubernetes platforms to ensure that the images are ready for deployment on multi-cloud environments.

Security measures in VMware Application Catalog

VMware Application Catalog helps secure the software supply chain for customers in several other ways as well.

Photon OS: A lightweight base image from VMware

VMware Photon OS is a Linux-based, open source, security-hardened, enterprise-grade appliance OS that is purpose-built for cloud and edge applications. It is a lightweight OS with fewer dependencies compared to other Linux distributions, where fewer dependencies typically mean fewer possibilities for security vulnerabilities. Customers get the option of using Photon OS as the base image for the OSS applications they procure from VMware Application Catalog.

The base image of OSS applications plays another critical role in minimizing the risk posed by upstream vulnerabilities. If the upstream vendor of an OSS releases a security patch, it's important that all the vulnerability fixes in that patch are included in the base OS image as well. Otherwise, the OSS application could remain unsecure despite the availability of a security patch. Photon OS being a VMware-maintained project provides us with the control we need over vulnerability response to ensure timely security fixes at the base OS level; and in turn, delivers secure OSS applications with minimal vulnerabilities. So Photon OS is the official recommended base image in VMware Application Catalog for customers who desire a zero CVE report from their CVE scanner. Photon OS, in combination with the VMware Application Catalog continuous upstream monitoring mechanism, can get you close to zero CVEs, and for some applications, we might even get an actual zero CVE report from scanners. Read more about how you can mitigate upstream vulnerabilities and improve compliance posture with Photon OS in VMware Application Catalog.

In addition to Photon OS, VMware Application Catalog provides the latest versions of third-party Linux distributions (e.g., Red Hat Universal Base Image, Ubuntu, and Debian) as base image options to offer our customers flexibility.

Software bill of materials delivered in SPDX format

All container images in VMware Application Catalog are delivered along with the corresponding software bill of materials (SBoM) in the Software Package Data Exchange (SPDX) format, an international open standard developed by the Linux Foundation for communication of SBoM information. The SBoMs from VMware Application Catalog help enterprises achieve compliance with National Telecommunications and Information Administration (NTIA) standards, as they contain details such as component hash, unique identifiers and dependency relationships of OSS applications as prescribed by the NTIA pursuant to United States Executive Order 14028. Users can also optimize and automate security-related decision-making processes by working with tools that can directly consume inputs using the SPDX format. Read more about using SBoMs from VMware Application Catalog.

Support for air-gapped environments

VMware Application Catalog is delivered as a software-as-a-service (SaaS) offering. Platform engineers request images via a user interface, but all continuously maintained, trusted open source building blocks are delivered to a user-defined or VMware-hosted private registry. In an air-gapped environment, all applications, networks and resources are physically isolated from external inputs to prevent potential security risks. With VMware Application Catalog, users have the option to directly retrieve images, charts and metadata, or replicate them to their own private registry. Additionally, applications with Photon OS as the base OS image are verified for functionality in air-gapped environments. Thus, customers seeking air-gapped deployments get verified, ready-to-use OSS applications from VMware Application Catalog. Read more about how to consume VMware Application Catalog images using a private Harbor registry, or read about how to synchronize Helm charts from VMware Application Catalog in air-gapped environments using the open source charts-syncer tool.

Vulnerability Exploitability eXchange (VEX)

VEX was developed as part of the National Telecommunications and Information Administration (NTIA) multistakeholder process for software component transparency. Often, the development, operations, and security teams working on a product are left trying to fix a vulnerability identified by a vulnerability scanner in an upstream component, without being fully aware of whether that vulnerability is actually exploitable in their final product. VEX solves this problem by providing information on whether a product is affected by a specific vulnerability in one of its upstream components and, if so, it provides additional information about identified remediation actions as well. This allows development and operations teams dealing with vulnerability management to quickly review their options and mitigate risks. VMware Application Catalog delivers VEX documentation for all container images built with Photon OS 4 as the base image. The machine readability of VEX enables

automation and supports integration with broader tooling and processes. Read more about using VEX documentation in VMware Application Catalog.

Containers, Helm charts and metadata signing with Cosign

All containers, Helm charts and metadata from VMware Application Catalog are signed using Sigstore Cosign before being delivered to Open Container Initiative (OCI)-compliant private registries. This essentially brings another layer of security to customers' OSS supply chains by providing authorship evidence; additional proof of provenance about where the image has come from, and the guarantee that the images, charts and metadata have not been tampered with, modified or altered in any form. To verify the signatures and be assured that the content they have received is from a trusted source, users can run a simple verification command in their local machine. See how in this documentation.

Best practices for securing and hardening containers and Helm charts

Over the years, Bitnami has gained respect and popularity for building industry standard best practices when it comes to securing and hardening container images. As the enterprise version of Bitnami Application Catalog, VMware Application Catalog leverages Bitnami expertise to ensure that all container images go through a standardized set of security and hardening procedures. This includes the generation of both rolling and immutable image tags, non-root configuration and arbitrary Universally Unique Identifiers (UUIDs), Common Vulnerability and Exposure (CVE) and virus scanning, verification and functional testing, compliance with Federal Information Processing Standards (FIPS), and minimizing container size and dependencies. Read more about each of these points in detail.

Non-root containers

Container images are run as root users by default. This means users or malicious code can carry out privileged tasks, such as installing system packages, editing configuration files, binding privilege ports, adjusting permissions, creating system users and groups, or accessing networking information. By contrast, with non-root images, conducting these types of privileged tasks is prohibited, so the containers are inherently more secure and are more appropriate for production environments. About 80 percent of VMware Application Catalog container images are built as non-root containers. This means that no malicious code can gain elevated permissions on the container host.

Also, some Kubernetes distributions, such as Red Hat OpenShift, run containers using random UUIDs. This approach is not compatible with root containers, which must always run with the root user's UUID. In such cases, root-only container images will simply not run. Non-root container images from VMware Application Catalog are compatible to run on every Kubernetes platform. Read more about how using non-root containers helps keep your application deployments secure.

Elevated security for Kubernetes secrets

For modern-day enterprises that manage their infrastructure configuration as code, it is challenging to keep sensitive information such as database passwords, OAuth tokens, SSH keys or Slack tokens in the form of Kubernetes secrets safe and secure within shared Git repositories. The sealed secrets resource addresses this challenge by enabling customers to add an asymmetric, cryptography-based protection to their Kubernetes secrets stored in shared repositories.

Sealed secrets is a popular open source project led by VMware's team focused on Bitnami, which has registered more than 700 million pulls in Docker Hub, with more than 200 million in the month of June 2023 alone. Sealed secrets are "one-way" encrypted secrets that can be created by anyone but that can be decrypted only by the controller running in the target cluster. Once a secret stored in a shared or public Git repository gets encrypted as a sealed secret and is uploaded to the target Kubernetes cluster, it remains fully safe and secure. Only the sealed secrets controller will be able to decrypt it with the private sealing key and recover the original secret, thus protecting sensitive data while still having them within shared repositories. By providing enterprise support for sealed secrets, VMware Application Catalog places customers in the best position to take advantage of a reliable and popular tool to secure their Kubernetes secrets and better control their Kubernetes deployments. Read more about using sealed secrets with VMware Application Catalog.

Learn more

Get more information about VMware Application Catalog with these resources:

- Product webpage
- Solution overview
- Technical product documentation
- A current list of applications supported by VMware Application Catalog
- Contact the team at app-catalog@vmware.com

Item No: Security Measures in VMware Application Catalog_white paper 9/23