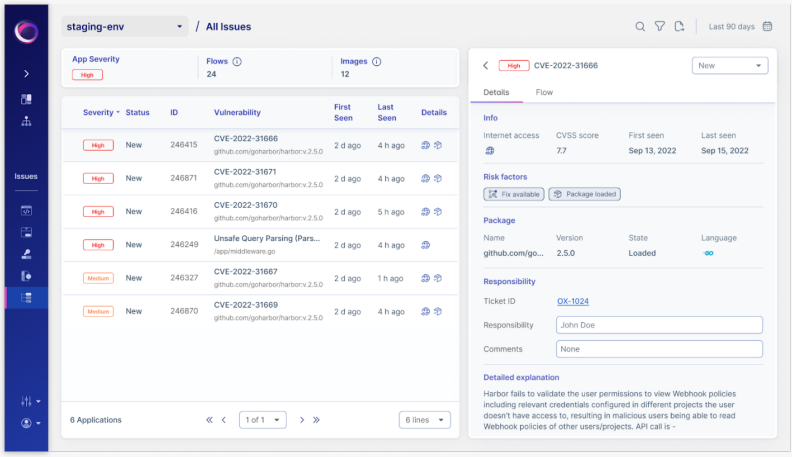
High Severity IDOR Vulnerabilities Identified by Oxeye Research Team in CNCF 'Harbor' Project by VMware

Newly Revealed High-Risk Vulnerabilities in Commonly Used Cloud Native Application Open-Source Security Project

TEL AVIV, ISRAEL, September 19, 2022 /EINPresswire.com/ -- Oxeye, the provider of award-winning cloud-native application security, today announced that its security researchers have uncovered several new high severity variants of the IDOR (Insecure Director Object Reference) vulnerabilities in CNCF-graduated project Harbor, the popular open-source artifact registry by VMware.

Oxeye Logo



IDOR

Harbor is an open-source cloud native registry project that stores, signs and scans content. It can integrate with various Docker registries to provide security features such as user management, access control and activity auditing.

Classified as an access control vulnerability, IDOR occurs when an application uses user-supplied input to access objects directly. IDOR is a high severity threat and is considered to be the most serious web application security risk on the most current OWASP top 10 list.

Access control systems are designed to enforce policies that prevent users from acting outside of intended permissions. Access control failures typically lead to unauthorized information disclosure, modification, data deletion, or the performance of business functions outside of a user's limits. In this research, IDOR was discovered in VMware's Harbor, which allows users to better manage their application artifacts. Role-based access control (RBAC) in place is usually a best practice against IDOR vulnerabilities, but this research tested that theory with surprising

results.

The IDOR vulnerability in Harbor leads to the disclosure of webhook policies without authorization. Harbor allows users to configure webhook policies to receive notifications about certain events in the repository, e.g., when a new artifact is pushed or when an existing one is deleted. Once a webhook policy is added, a Harbor user may view details of the created webhook policies. In this example, the vulnerability occurred because Harbor only attempted to validate that the requesting user had access to the project ID specified in the request. But it failed to validate that the requested webhook ID belonged to the specified project ID.

Another IDOR variant leads to the disclosure of job execution logs. P2P (peer-to-peer) preheating allows Harbor users to integrate with P2P engines such as Dragonfly or Kraken to distribute Docker images at scale. By combining this IDOR vulnerability with the "ParseThru" vulnerability identified previously by the Oxeye research team, an attacker may have the ability to read Docker image layers to which they lack access credentials.

The following IDOR CVE numbers link back to GitHub and are associated with the vulnerabilities mentioned above.

- CVE-2022-31671 - https://github.com/goharbor/harbor/security/advisories/GHSA-3wpx-625q-22j7
- CVE-2022-31666 - https://github.com/goharbor/harbor/security/advisories/GHSA-jf8p-3vjh-pq94
- CVE-2022-31670 - https://github.com/goharbor/harbor/security/advisories/GHSA-3637-v6vq-xqqw
- CVE-2022-31669 - https://github.com/goharbor/harbor/security/advisories/GHSA-8c6p-v837-77f6
- CVE-2022-31667 - https://github.com/goharbor/harbor/security/advisories/GHSA-xx9w-464f-7h6f

"While role-based access control (RBAC) is important for maintaining a strong security position, it is not the end-all for absolute system defense against IDOR vulnerabilities," said Ron Vider, CTO and Co-founder, Oxeye. "As revealed by Oxeye security researchers Gal Goldshtein and Daniel Abeles, implementing more robust practices that include setting strict roles for API endpoints, simulating threat actors to test those roles in an attempt to break permission models, and avoiding property duplication to maintain a single source of truth can ensure resiliency."

All IDOR variants mentioned in this announcement have been communicated to the VMware Security Response and Harbor Engineering teams, who promptly collaborated towards a quick and effective resolution. All have been addressed (fixed) in the latest version of Harbor. For additional information on the IDOR vulnerability in Harbor, please visit the Oxeye security blog at https://www.oxeye.io/blog/guess-whos-rbac.

"The quality of the open source software and commercial distributions we and our partners

distribute is vital to us and to the organizations that use it. We are grateful to Oxeye and its researchers for their diligence in finding vulnerabilities and their excellent collaboration in helping us address them." – Roger Klorese, Product Line Manager, Project Harbor, VMware

Oxeye customers can leverage the Oxeye cloud-native security platform to detect and mitigate these IDOR vulnerabilities.

If you are interested in learning more about how Oxeye can assist with cloud native application security challenges, please visit https://www.oxeye.io/get-a-demo to register for a demonstration.

Resources:
- Follow Oxeye on Twitter at @OxeyeSecurity
- Follow Oxeye on LinkedIn at https://www.linkedin.com/company/oxeyeio/
- Visit Oxeye online at http://www.oxeye.io

About Oxeye
Oxeye provides a cloud-native application security solution designed specifically for modern container and Kubernetes-based architectures. The company enables customers to quickly identify and resolve all application-layer risks as an integral part of the software development lifecycle by offering a seamless, comprehensive, and effective solution that ensures touchless assessment, focus on the exploitable risks, and actionable remediation guidance. Built for Dev and AppSec teams, Oxeye helps to shift security to the left while accelerating development cycles, reducing friction, and eliminating risks. To learn more, please visit www.oxeye.io.

- END -

Dean Agron
Oxeye
+972 54-672-2465
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
