oxsecurity

Attack Path Reachability Analysis

Distilling fragmented AppSec data into unified action

The Challenge

Despite advancements in security tooling, the frequency of software supply chain attacks has surged, increasing by 742% from 2019 to 2022. Application Security (AppSec) teams continue to face significant challenges, including limited visibility, manual tasks, and poor coordination. These issues are exacerbated by the rapid pace of development cycles and the broad scope of modern applications, APIs, and cloud environments, underscoring the need for a systematic and actionable approach to understanding and responding to attacker behaviors and techniques within the software supply chain.

The OX Solution

OX Security's Attack Path Reachability Analysis, part of the industry's first Active ASPM platform, provides a single-interface solution that goes beyond detecting vulnerabilities to offer a comprehensive understanding of potential attack paths. Covering attack vectors like third-party library vulnerabilities, build and deployment system attacks, and compromised software updates, the Attack Path Reachability Analysis also addresses concerns across Code, API's and Cloud environments. By visualizing and mapping these paths, it allows users to view security from an adversary's perspective, turning strategic insights into actions that prioritize critical reachable issues over hygiene issues, thereby significantly enhancing risk mitigation and fortifying security posture.

Comprehensive Vulnerability Insights for Effective Threat Modeling: Detailed visualizations, provides users the insight needed to dissect potential attack vectors, entry points, data flows, and the likely progression of an attacker from code through API, and cloud.

Targeted Issue Prioritization Based on Reachability, Applicability, and Exploitability: Through proprietary data collection, consolidation, enrichment, and analysis, risks are meticulously prioritized based on reachability, applicability, and exploitability.

Holistic Issue Review and Enhanced Analysis: Three tailored levels of security analysis — Code, API, and Cloud — are integrated into one comprehensive evaluation.

Cloud Monitoring and Artifact Management: The platform enables users to efficiently monitor and verify the operational status of containers in the cloud by systematically tagging applications based on their internet exposure and tracking artifacts to accurately assess the application's integrity.

Key Benefits

SECURE YOUR APPLICATIONS WITH ADVANCED REACHABILITY INSIGHTS

By integrating Code, APIs, and Cloud with the function call graph, OX uncovers hidden vulnerabilities and secure potential breach points, providing a layer of protection that positions your enterprise ahead of threats.

UNDERSTAND YOUR EXPOSURE AND SWIFTLY REMEDIATE VULNERABILITIES

Clarity in crisis is essential. The Attack Path Reachability Analysis not only helps AppSec teams understand the nuances of each threat but also the reasoning behind its assessed severity. This deep insight into reachability streamlines the triage process, ensuring that every response is as informed as it is quick.

EMPOWER YOUR APPSEC TEAMS TO FOCUS ON CRITICAL ISSUES EFFICIENTLY

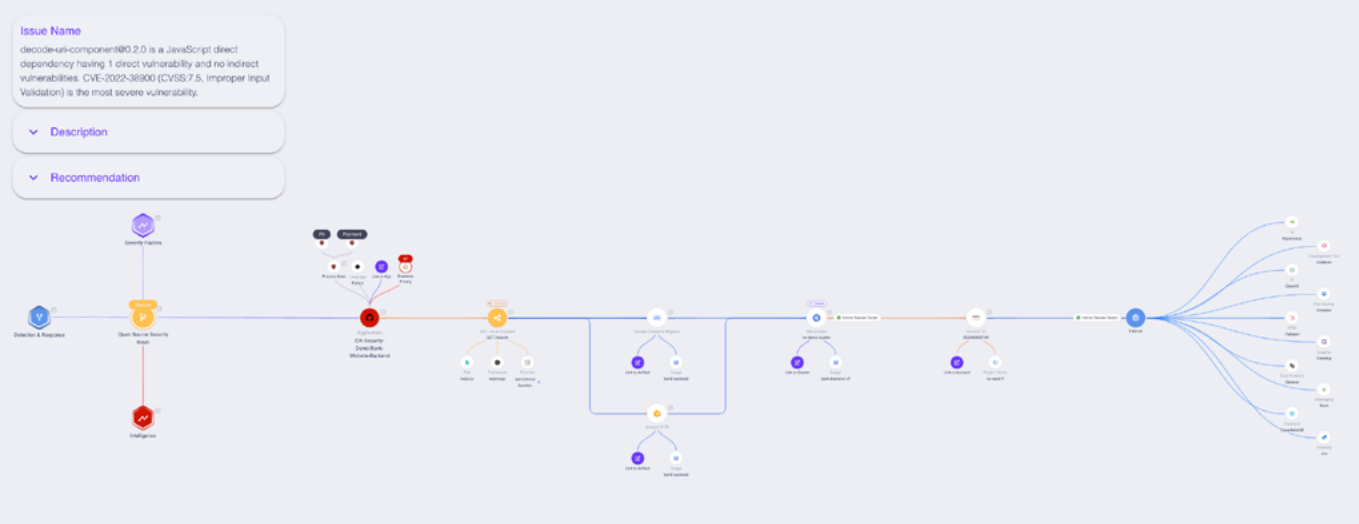
Distinguishing critical issues from trivial ones is not just necessary—it's a strategic advantage. The Attack Path Reachability Analysis transforms how your AppSec teams identify, respond to, and remediate threats. By highlighting the most critical risks in Code, API, and Cloud environments, we ensure your team's efforts are focused, impactful, and timely.

EFFECTIVELY MANAGE THIRD-PARTY INCIDENTS

Ensuring that users have instant access to the latest inventories saves a great deal of time. Enhanced BOM capabilities deliver a thorough review of libraries, API usage, and SaaS dependencies. This comprehensive inventory management system not only mitigates surprises but also minimizes manual tracking errors.

MOBILIZE TEAMS THROUGH DATA

Effective collaboration relies on clear communication. The Attack Path Reachability Analysis serves as a common language among security, development, DevOps, and operations teams. It makes the severity and details of security issues accessible and comprehensible to everyone involved. By demystifying the technical aspects, we cultivate a collaborative environment that accelerates resolution and strengthens resilience.



INTERESTED IN LEARNING MORE VISIT: WWW.OX.SECURITY/BOOK-A-DEMO/

ox security