SOLUTION BRIEF

AppSec Vulnerability Prioritization by OX: From Alert Fatigue to Action

Challenge

According to recent research from OSC&R, 84% of applications have at least one vulnerability, and about 46% of these vulnerabilities are considered high severity. However, the challenge lies in the fact that only 35% of organizations have a standardized process for vulnerability prioritization across different environments such as code, applications, and cloud resources.

Lack of Business Context

Unclear Fix Impact and Efficacy

Disparate Team Views

Reachability Context

Today's organizations need more than notifications and deduplication; they require prioritization based on reachability, exploitability, and impact, which also incorporates threat, environmental, and business context. With consolidated views and the ability to remediate swiftly, organizations can significantly enhance the effectiveness of their AppSec programs, reduce the backlog of vulnerabilities, and focus on actual risk.

Introducing a Strategic Approach to Managing Security Risks

OX Security's AppSec Vulnerability Prioritization incorporates a tailored framework enhanced by our Attack Path Analysis, transforming the management of vulnerabilities. This strategic approach enables our customers to precisely target and address the most critical vulnerabilities, optimizing the allocation of resources and strengthening their security defenses.

With OX you'll achieve:

Comprehensive Vulnerability Management and Prioritization: Ensure a thorough and efficient approach to managing vulnerabilities by grouping and prioritizing all vulnerabilities by infrastructure, applications, code, and root cause. This holistic strategy enhances overall security posture and resource allocation.

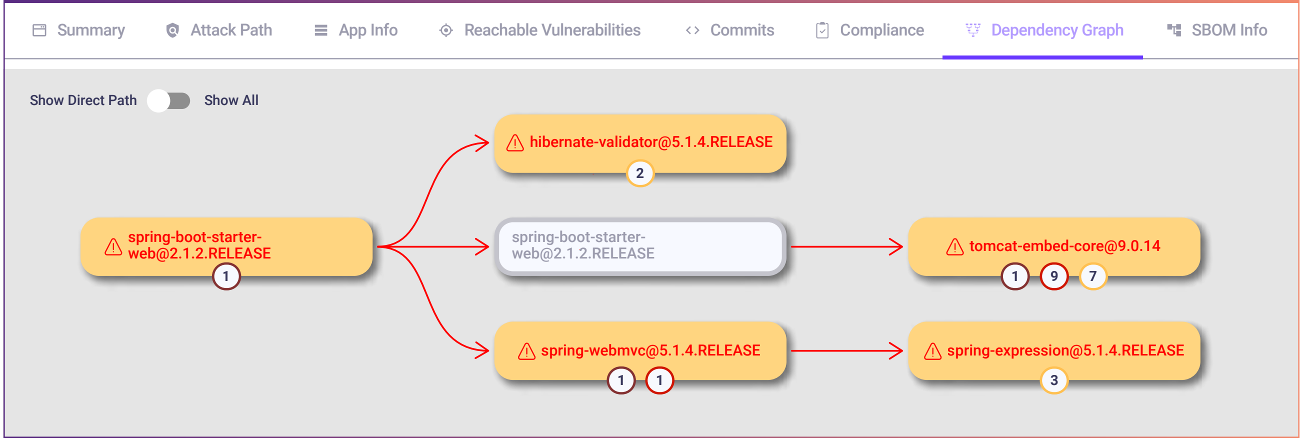
Targeted Issue Prioritization: Meticulously prioritize risks through proprietary data collection, consolidation, enrichment, and analysis, focusing on reachability, applicability, and exploitability. This precision ensures that critical threats are addressed promptly and effectively.

Alert and Noise Reduction: Overcome alert fatigue and enhance focus on critical threats by reducing alerts and clarifying risk priorities through active data collection. This streamlined approach safeguards your organization by emphasizing the most pressing security issues.

Proactive Remediation: Prevent recurring security issues and boost overall security efficiency by addressing vulnerabilities at their source. This proactive approach minimizes future risks and enhances long-term protection.

Effective Zero-Day Vulnerability Response: Fortify your defenses against zero-day vulnerabilities like Log4shell by automatically analyzing issues at the root cause level. Identify which artifacts in the SDLC introduce vulnerabilities and determine the responsible code owners, ensuring rapid and effective mitigation.

Leveraging all available information, OX investigates the details of each item and maps the dependencies between multiple security issues into a single, actionable alert.


Summary
Attack Path
App Info
Reachable Vulnerabilities
Commits
Compliance
Dependency Graph
SBOM Info
Show Direct Path
Show All
hibernate-validator@5.1.4.RELEASE
2
spring-boot-starter-web@2.1.2.RELEASE
1
spring-boot-starter-web@2.1.2.RELEASE
tomcat-embed-core@9.0.14
1
9
7
spring-webmvc@5.1.4.RELEASE
1
1
spring-expression@5.1.4.RELEASE
3

Straight Forward Visibility and Prioritization

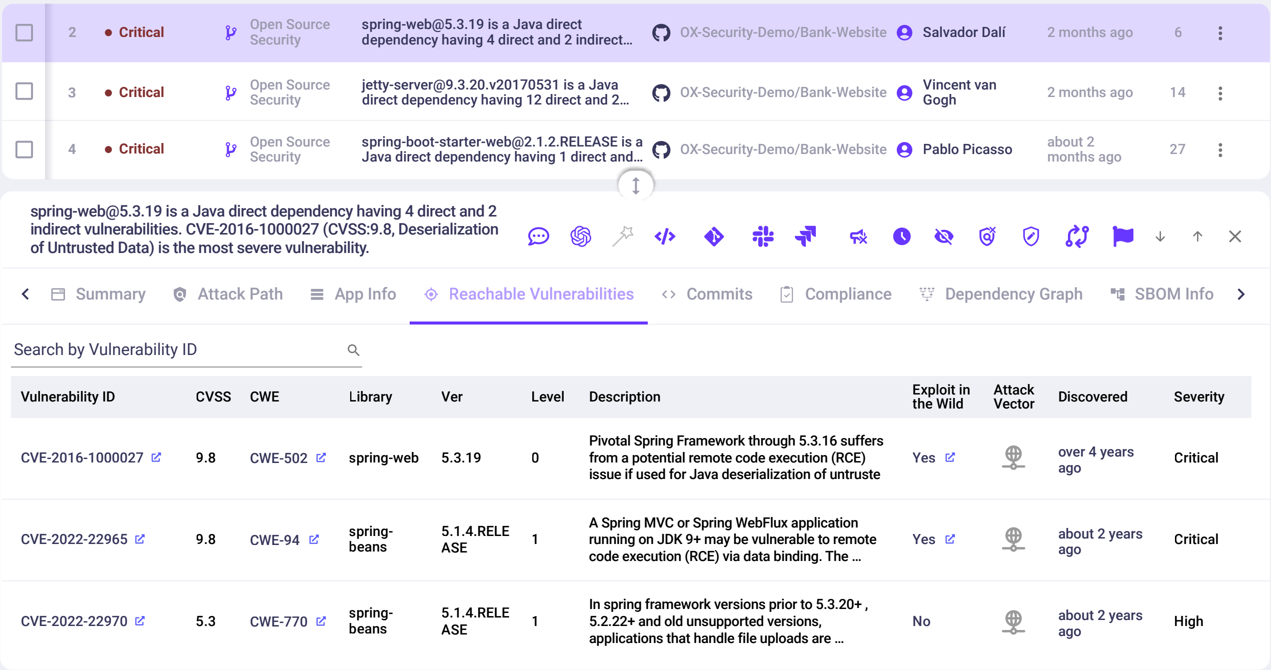
OX Security delivers unified security visibility, making it easier for all teams to agree on the priority order of fixes and the next steps to remediate. By leveraging comprehensive data and advanced analysis, OX enhances the efficiency and effectiveness of vulnerability management. **Key features that enable this streamlined approach include:**

Out-of-the-Box Prioritization: Offers default priority views, including a list of security issues sorted by shared root cause and fix impact. This feature accelerates the initial setup and provides a solid foundation for vulnerability management.

Custom Prioritization Logic: Provides custom prioritization logic with a wide range of filters to sort vulnerabilities by severity, exploit status, resource type, detection tool, business impact, and more. This flexibility ensures that prioritization aligns with specific business objectives and risk appetite.

Consolidated Issue Analysis: Aggregates vulnerabilities across domains and conducts root cause analysis. This approach consolidates multiple vulnerabilities into a single, actionable issue, dramatically reducing alert fatigue and aiding in prioritization.

OX reduces the volume of alerts and simplified remediation by consolidating all of the vulnerabilities contributing to the root cause of a security issue.



□	2	● Critical	Open Source Security	spring-web@5.3.19 is a Java direct dependency having 4 direct and 2 indirect…	OX-Security-Demo/Bank-Website	Salvador Dalí	2 months ago	6	⋮
□	3	● Critical	Open Source Security	jetty-server@9.3.20.v20170531 is a Java direct dependency having 12 direct and 2…	OX-Security-Demo/Bank-Website	Vincent van Gogh	2 months ago	14	⋮
□	4	● Critical	Open Source Security	spring-boot-starter-web@2.1.2.RELEASE is a Java direct dependency having 1 direct and…	OX-Security-Demo/Bank-Website	Pablo Picasso	about 2 months ago	27	⋮

spring-web@5.3.19 is a Java direct dependency having 4 direct and 2 indirect vulnerabilities. CVE-2016-1000027 (CVSS:9.8, Deserialization of Untrusted Data) is the most severe vulnerability.

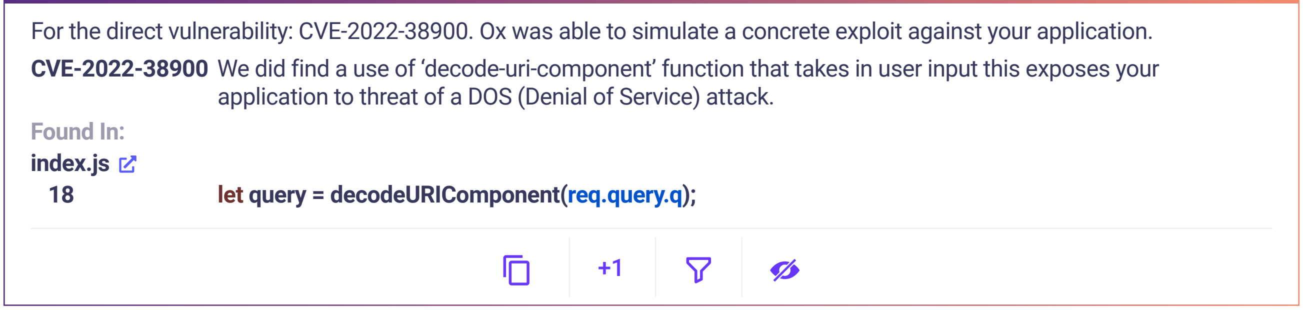
Search by Vulnerability ID

Vulnerability ID	CVSS	CWE	Library	Ver	Level	Description	Exploit in the Wild	Attack Vector	Discovered	Severity
CVE-2016-1000027	9.8	CWE-502	spring-web	5.3.19	0	Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untruste	Yes		over 4 years ago	Critical
CVE-2022-22965	9.8	CWE-94	spring-beans	5.1.4.RELEASE	1	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The …	Yes		about 2 years ago	Critical
CVE-2022-22970	5.3	CWE-770	spring-beans	5.1.4.RELEASE	1	In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are …	No		about 2 years ago	High

Context-Sensitive Prioritization: Maximizes accuracy in prioritizing identified issues by applying a 3-layer contextual analysis. Each issue is analyzed based on reachability (can an attacker access the vulnerability), exploitability (if it is reachable, can the attacker take advantage of it), and damage (is malicious behavior such as remote code execution possible by exploiting the vulnerability).

For example, if a vulnerable library is incorporated into an application codebase but not used in an exploitable way, OX's prioritization assigns a lower severity score. Other tools do not apply this context and, therefore, cannot accurately assess and prioritize the risk.

Although this dependency was imported into the code, it is not actually being used and therefore poses a LOW risk rather than CRITICAL. OX's automated triage has identified this library is being used in a way that poses a legitimate security risk.



For the direct vulnerability: CVE-2022-38900. Ox was able to simulate a concrete exploit against your application.

CVE-2022-38900 We did find a use of 'decode-uri-component' function that takes in user input this exposes your application to threat of a DOS (Denial of Service) attack.

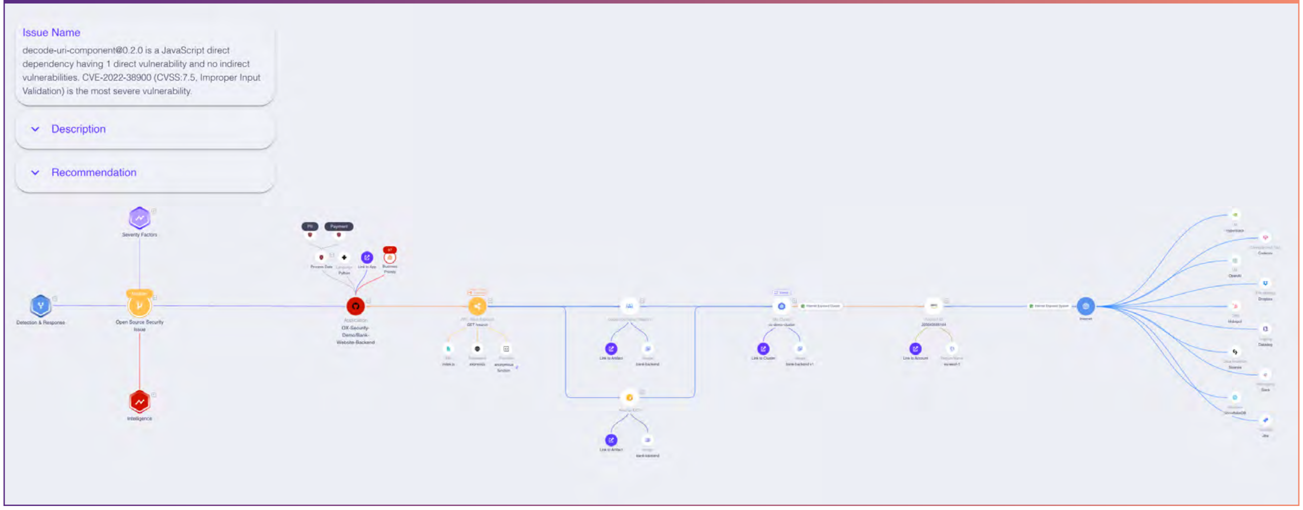
Found In:

index.js

```
18    let query = decodeURIComponent(req.query.q);
```

Exposure Analysis: Includes the origin of the vulnerability, its downstream impacts, and whether it is actively being exploited. This comprehensive view enables more informed decision-making and effective prioritization.

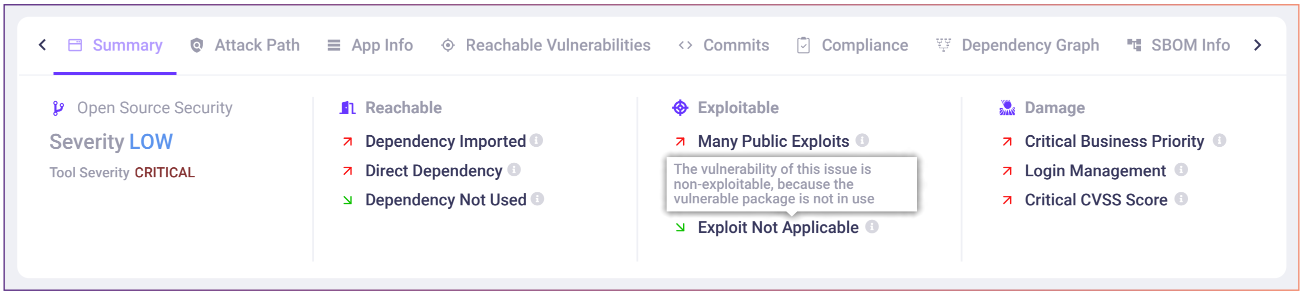
OX's contextual prioritization and enrichment based on attack path analysis



Issue Name

decode-uri-component@0.2.0 is a JavaScript direct dependency having 1 direct vulnerability and no indirect vulnerabilities. CVE-2022-38900 (CVSS:7.5, Improper Input Validation) is the most severe vulnerability

Contextual Enrichment: Incorporates unique context such as reachability to help prioritize vulnerabilities more effectively. This reduces the burden on security professionals and ensures resources are focused on the most critical threats.



Summary | Attack Path | App Info | Reachable Vulnerabilities | Commits | Compliance | Dependency Graph | SBOM Info

Open Source Security
Severity LOW
Tool Severity CRITICAL

Reachable
↗ Dependency Imported
↗ Direct Dependency
↘ Dependency Not Used

Exploitable
↗ Many Public Exploits
The vulnerability of this issue is non-exploitable, because the vulnerable package is not in use
↘ Exploit Not Applicable

Damage
↗ Critical Business Priority
↗ Login Management
↗ Critical CVSS Score

Comprehensive Issue Management: Enriches issue reports with Software Bill of Materials (SBOM) information, including licensing, maintenance status, popularity, and code usage details. Extends analysis for containerized applications to base image vulnerabilities, offering comprehensive insights based on the Dockerfile. By recommending base image upgrades, helps resolve multiple vulnerabilities simultaneously, significantly reducing the attack surface.

No-Code Workflows and Custom Rules: Offers no-code capabilities that allow users to easily define their own business logic. This empowers organizations to tailor the prioritization process to their specific needs without requiring deep technical expertise.

Remediation-Focused Issue Resolution: Prioritizes remedy over mere problem identification. Streamlines the remediation process by consolidating issues based on their solutions rather than treating each problem separately. This method ensures that efforts are focused on effective vulnerability prioritization and management, specifically tailored by context for more targeted root cause analysis.

Extensive Integration Capabilities: Supports 100+ connectors to industry commercial tools. Additionally, home-grown scanning tools enhance both vulnerability detection and contextual analysis. This dual approach ensures comprehensive coverage and deeper context, forming the basis of effective prioritization.

WIZ
aws
JFrog

Enhance Your Security Posture

By leveraging the OX Attack Path and our comprehensive prioritization approach, OX Security empowers organizations to focus on what matters most, ensuring efficient and effective vulnerability management. This enables our customers to protect their critical assets and maintain a strong security posture. For more insights and detailed implementation steps, visit our website.

> "Prior to OX, we were drowning in a sea of alerts. The platform's ability to prioritize vulnerabilities based on context has been a game-changer. Now, we can effectively target the risks that pose the greatest threat to our business."
>
> **Eli Rapport**
> CISO, Moovit

About OX Security

At OX Security, we're simplifying application security (AppSec) with the first-ever Active ASPM platform offering seamless visibility and traceability from code to cloud and cloud to code. Leveraging our proprietary AppSec Data Fabric, OX delivers comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. Recently recognized as a Gartner Cool Vendor and a SINET 16 Innovator, OX is trusted by dozens of global enterprises and tech-forward companies. Founded by industry leaders Neatsun Ziv, former VP of CheckPoint's Cyber Security business unit, and Lior Arzi from Check Point's Security Division, OX's Active ASPM platform is more than a platform; it empowers organizations to take the first step toward eliminating manual AppSec practices while enabling scalable and secure development.

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

oxsecurity