OWASP Makes Significant Advancements in SBOM Effectiveness and Risk Prioritization

Adds support for exploit prediction, VEX, and non-public vulnerabilities to OWASP Dependency-Track, an SBOM analysis platform, relied on by thousands of organizations, analyzing over 200M components monthly.

Wakefield, Massachusetts May 18, 2022 (Issuewire.com) - The Open Web Application Security Project (OWASP), the worldwide nonprofit organization focused on improving the security of software, today announced significant advancements necessary to operationalize the software bills of materials pursuant to U.S. Executive Order 14028.

OWASP Dependency-Track, the leading SBOM analysis platform, introduced three new capabilities necessary to improve the efficiency and effectiveness of SBOM vulnerability management.

Statistics show that upwards of 90% of vulnerable components are not exploitable in the context of a given system or application. In response, Vulnerability Exploitability eXchange (VEX) provides a way for software suppliers to communicate exploitability information to consumers. VEX provides consumers insight into the vulnerable components that pose risk, and the ones that don't. Dependency-Track now fully supports the OWASP CycloneDX VEX format, one of two recognized VEX formats identified by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Dependency-Track is the first open platform that facilitates the creation and consumption of VEX between software suppliers and consumers.

With today's release, OWASP also announced that Dependency-Track now fully supports exploit prediction via the Exploit Prediction Scoring System (EPSS), an open data-driven effort for estimating the likelihood that software vulnerabilities will be exploited in the wild.

"VEX and EPSS are a powerful combination that allows organizations to focus on the vulnerabilities that matter when they matter," says Steve Springett, founder, and co-leader of the OWASP Dependency-Track project. "It's incredibly important that organizations have the intelligence and tools necessary to effectively respond to the next high-profile vulnerability. We're excited to bring these capabilities to Dependency-Track for the benefit of all".

Today's release also adds private vulnerability database support to Dependency-Track allowing organizations to identify vulnerabilities in internally-developed components.

Modular application development is common across enterprises. Components are often reused across multiple applications internal to an organization. These reusable components may often contain vulnerabilities identified through best practices such as static code analysis or fuzzing. With today's release, vulnerable internally-developed components are now identifiable via SBOM.

"Communicating and tracking vulnerabilities affecting internally-developed components can be a challenge, especially in larger organizations. Many processes today are primarily focused on tracking OSS risk. However, the reality is that custom code can be just as vulnerable as third-party code, with the potential of affecting large parts of an organization's application landscape" says Niklas Düster, co-leader of the OWASP Dependency-Track project. "We believe the addition of a private vulnerability database to be immensely useful, as it will allow organizations to reuse existing processes and automation to drive remediation efforts".

Visit https://docs.dependencytrack.org/usage/executive-order-14028/ to learn how OWASP Dependency-Track helps organizations and governments support U.S. Executive Order 14028.

Visit https://dependencytrack.org/ to get started.

Media Contact

OWASP Foundation

steve.springett@owasp.org

Source : OWASP

See on IssueWire