



Over 244,000 vulnerabilities tracked, representing 57,000 products & 27,000 Vendors

Your only source for Vulnerability Timeline and Exposure Metrics (VTEM)

Five-Star rating system ranks software products and publishers

Over 79,000 vulnerabilities NOT found in CVE/NVD

Continual updates by an expert research team

Contact Risk Based Security

3308 W Clay St,
Richmond, VA 23230

(855) RBS-RISK

sales@riskbasedsecurity.com

www.riskbasedsecurity.com

vulndb.cybersecurity.com



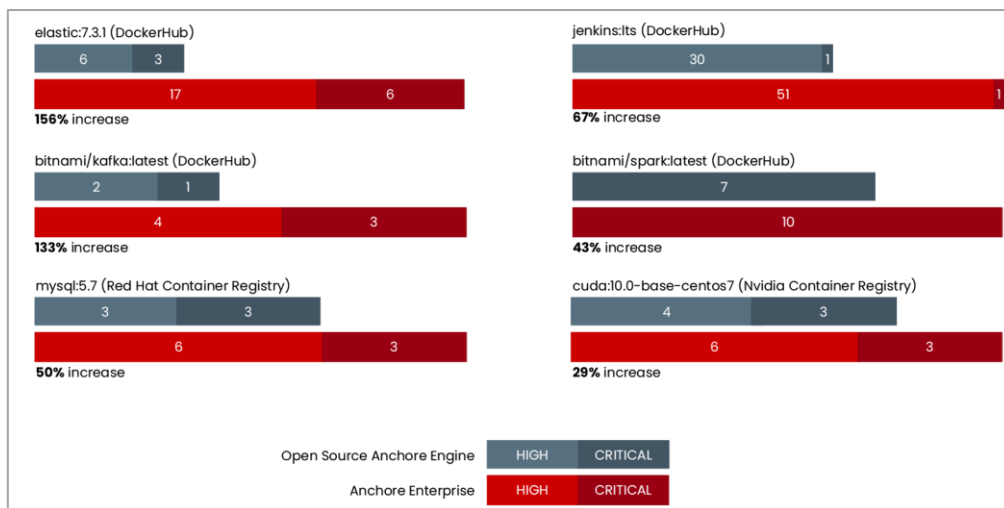
Enhanced Vulnerability Data for Anchore Enterprise Users

Anchore Enterprise users can benefit from an extra layer of security by using the VulnDB® integration, which allows organizations to analyze container images at any point in the development process. With functionality now available in Anchore Enterprise, customers have access to enhanced vulnerability data from VulnDB* for increased fidelity, accuracy, and timeliness of image vulnerability scanning results.

Our VulnDB database has over 244,000 vulnerabilities and covers more than 25,000 vendors, 2,000 OSS/third-party libraries and has over 79,000 vulnerabilities that are not found in CVE or NVD. The VulnDB integration in Anchore Enterprise gives customers deeper metadata that may not be found in the public source and allows development, security, and operations teams to make more informed vulnerability and policy management decisions around their container image workloads at any point in the CI/CD pipeline.

Key integration benefits include:

- Enhanced viewing of vulnerability data within the Anchore UI.
- Detailed metadata for VulnDB entries providing more information about the issue, including links to external sources.
- Enhanced feed for Anchore Enterprise users that gives customers access to our comprehensive database of over 244,000 vulnerabilities.



Comparison of the deltas between Anchore Engine (no VulnDB) and Anchore Enterprise (with VulnDB)

Get more information about the VulnDB Integration for Anchore Enterprise here:

<https://anchore.com/enhanced-vulnerability-data/>

* VulnDB subscription required