

Streamline and Save Time: One Platform to Inform Your Next Security Move

Uncover the potential risks in your tech stack all in one platform and make an informed security plan.

Overview

Researching potential risks in your technology stack is time-consuming and challenging, with results that are often scattered, inaccessible, and not clearly actionable. Cobalt now offers an effective way to navigate this task and make informed decisions.

Cobalt's Pentest as a Service platform now integrates with MITRE's CVE (Common Vulnerabilities and Exposures) list to enrich your asset data with known vulnerabilities and security exposures. Additionally, Cobalt's Risk Advisory Integration feature consolidates with the NVD's CPE (Common Platform Enumeration) database to ensure universal naming standards and clear, consumable information.

These additions empower you to level up your threat assessment process, while making it easier for stakeholders across the organization to understand security planning needs.

Key Benefits



Easy and Specific

Automated search functionality returns findings that relate to your specific assets.



Open and Collaborative

Risk advisory findings filter directly into the Cobalt platform in an easy-to-read table which provides a transparent view of current findings and a reference of historical findings.



Actionable and Clear

Links to access patches, hotfixes, and risk advisory findings give you actionable and clear next steps.

Offering Details

Associated pentests (20) Potential Vulnerabilities (16)

Based on automated process we were able to find 16 vulnerabilities on this asset in the National Vulnerability Database

Filter by criticality Vulnerability search

Vuln ID	CVSS Severity	Summary	Vulnerability report
CVE 2021 - 32036	High	An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions.	Vulnerability report
CVE 2021 - 32036	High	An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions.	Vulnerability report
CVE 2021 - 32036	High	An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions.	Vulnerability report
CVE 2021 - 32036	High	An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions.	Vulnerability report

Automation that Saves You Time

Automatically search the CVE for tailored risk advisories based on your assets. Rather than spending time sifting through layers of listings, the CVE integration streamlines your research, saving you time. You can focus on completing current tasks without compromising future planning.

Assets

New Asset

Title	Type	Attachment(s)	Potential Vulnerabilities	Total Pentest	Action
1234 Test	Mobile	3	<ul style="list-style-type: none">Low: 1Medium: 16High: 4 21	26	...

Platform-Based Advisories and Historical Data

A single information point for common vulnerability advisories to increase your organization's collaboration. Your Risk Advisory findings are housed right in the Cobalt platform. This means there is a single source of truth accessible to all stakeholders without extra cost: everyone has access to data at every step.

Associated Pentests Risk Advisory

Important: These risk advisories don't belong to your pentest. These are potential risks based on the Common Vulnerabilities and Exposures (CVE) standard. Select a vulnerability to view more details on the National Vulnerability Database (NVD) website.

Vulnerability ID	CVSS Severity	Technology
CVE-2021-28879	7.5 High	rust-lang Rust 1.51.0
CVE-2022-28738	7.5 High	Ruby-lang Ruby 3.1.0
CVE-2021-31162	7.5 High	rust-lang Rust 1.51.0
CVE-2017-9120	7.5 High	PHP 7.4.19
CVE-2021-21703	6.9 Medium	PHP 7.4.19
CVE-2022-31625	6.8 Medium	PHP 7.4.19
CVE-2021-21708	6.8 Medium	PHP 7.4.19
CVE-2021-29922	6.4 Medium	rust-lang Rust 1.51.0
CVE-2020-36323	6.4 Medium	rust-lang Rust 1.51.0
CVE-2022-31626	6 Medium	PHP 7.4.19
CVE-2022-24329	5 Medium	JetBrains Kotlin 1.3.30
CVE-2020-29582	5 Medium	JetBrains Kotlin 1.3.30

Access to Further Details and Remediation Options

Enhance your find-to-fix cycles with easy-to-access guidance. Your CPE and CVE data is consolidated into one easy-to-read table, ensuring that you are using globally recognized naming conventions. This enables you to dive deeper into Risk Advisories so you can better understand needed next steps, and plan for future fixes.



Ready to Get Started?
Request a Demo Today!



f in t i y c cobalt.io