censys

CVE Context in Censys Search

Unleash the Power of CVE Data

Common Vulnerabilities and Exposures (CVE) data is a critical resource for security operations and threat response teams who need to be able to act on timely and accurate vulnerability information. CVE Context in Censys Search intuitively integrates this valuable data into the Censys experience, unlocking game-changing vulnerability management capabilities. With CVE Context, you can prioritize remediation efforts, receive timely insights into vulnerable infrastructure, understand potential attack vectors, and reduce risks.

KEY USE CASES

Identify Outdated Software and Known Vulnerabilities

Quickly find hosts with outdated software or known vulnerabilities to help assess and prioritize risk levels effectively.

Enhance Threat Research

Dive deep into attack surfaces and cybersecurity trends to craft proactive defenses for detailed vulnerability assessments.

Monitor for New Vulnerabilities

Continuously monitor for new vulnerabilities or changes in software status to enable swift responses to potential threats.

Protect Critical Systems

Gain visibility into both IT and OT systems to proactively identify and remediate vulnerabilities, safeguarding essential services and national security interests.

Streamline Operations

Consolidate vulnerability information into a single platform to improve decision-making and threat management efficiency.

Censys discovers 3x more hosts with CVEs than the nearest competitor.

Rich with fields like CVE ID, Attack Complexity, Attack Vector, Privileges Required, CVSS Score, and KEV Information, CVE Context in Censys Search equips you with the critical, detailed data you need to ahead of threats and protect your organization.

CVE Context Use Cases & Queries

The following use cases and corresponding queries illustrate just some of the many ways CVE Context can be leveraged in practice.

Use Case	Query
Find hosts with critical-scored vulnerabilities with low attack complexity ratings.	`cves.cvss.score: [9 to 10] and cves.cvss.components.attack_complexity="LOW"`
Find hosts with CVEs that are known exploited vulnerabilities.	`cves.cvss.score: [9 to *] and cves.kev: *`
Find hosts with known exploited vulnerabilities added within the past month.	`cves.kev.date_added: [now-1M to *]`
Find hosts with critical vulnerabilities that attackers can easily exploit.	`cves.cvss.score: [9 to 10] and cves.cvss.components.privileges_required="NONE" and cves.cvss.components.attack_complexity="LOW"`

Consider combining these queries with IP ranges or other information to focus results on the resources that are of specific interest to you.

Get Started Today

Ready to harness the power of CVE Context for yourself? Check out our CVE Context tutorial and reach out to your Censys Customer Success Manager to learn more!