censys

CVEs as Risks in Censys ASM

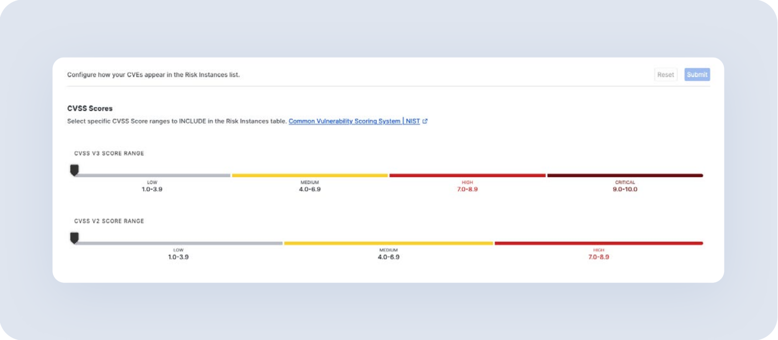
Expand Vulnerability Discovery to Your Attack Surface

As cybersecurity threats grow in complexity and frequency, gaining complete visibility into external vulnerabilities is more critical than ever. **CVEs as Risks in Censys ASM** addresses this need by enabling you to efficiently detect and prioritize vulnerabilities across your attack surface. By providing metrics like CVSS, KEV, and EPSS, this feature ensures that you can focus your efforts on the most severe and exploitable risks.

Key Benefits

Broader Coverage

Gaining complete visibility into your vulnerabilities is essential to prevent blind spots in your security. Censys does this by automatically mapping detected software to associated CVEs across your entire attack surface.



Configure how your CVEs appear in the Risk Instances list.

CVSS Scores

Select specific CVSS Score ranges to INCLUDE in the Risk Instances table. Common Vulnerability Scoring System | NIST

CVSS V3 SCORE RANGE

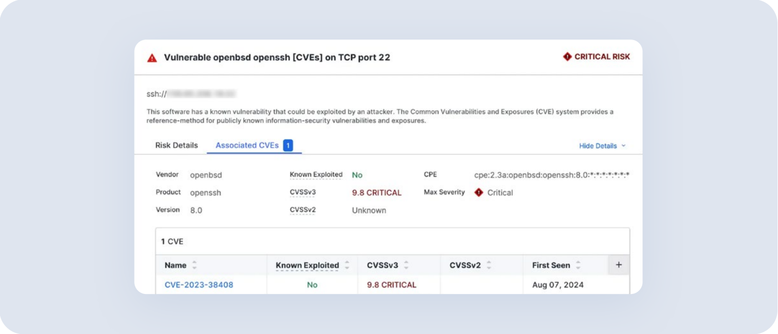
LOW	MEDIUM	HIGH	CRITICAL
1.0-3.9	4.0-6.9	7.0-8.9	9.0-10.0

CVSS V2 SCORE RANGE

LOW	MEDIUM	HIGH
1.0-3.9	4.0-6.9	7.0-8.9

Prioritize with Precision

Focusing on the most critical vulnerabilities saves time and mitigates the highest risks. Censys leverages CVSS, KEV, and EPSS metrics to prioritize based on severity and exploitability.



Vulnerable openbsd openssh [CVEs] on TCP port 22 — CRITICAL RISK

ssh://[redacted]

This software has a known vulnerability that could be exploited by an attacker. The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

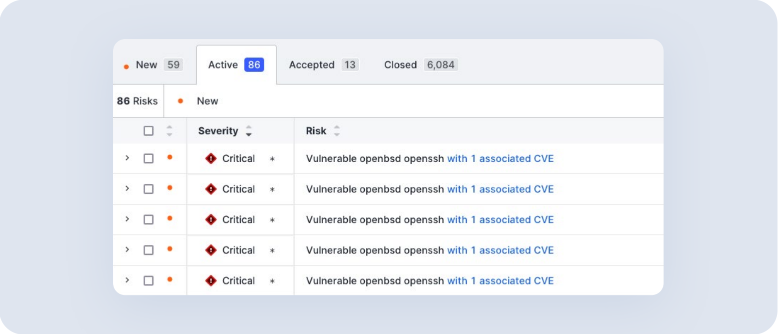
Vendor	openbsd	Known Exploited	No	CPE	cpe:2.3a:openbsd:openssh:8.0:*:*:*:*:*:*
Product	openssh	CVSSv3	9.8 CRITICAL	Max Severity	Critical
Version	8.0	CVSSv2	Unknown		

1 CVE

Name	Known Exploited	CVSSv3	CVSSv2	First Seen
CVE-2023-38408	No	9.8 CRITICAL		Aug 07, 2024

Unmatched Detection

Responding quickly to emerging threats is crucial for minimizing exposure. Censys provides real-time tracking of new CVEs and identifies vulnerabilities as soon as new software is detected—no deep scanning required.



86 Risks ● New

	Severity	Risk
› □ ●	Critical *	Vulnerable openbsd openssh with 1 associated CVE
› □ ●	Critical *	Vulnerable openbsd openssh with 1 associated CVE
› □ ●	Critical *	Vulnerable openbsd openssh with 1 associated CVE
› □ ●	Critical *	Vulnerable openbsd openssh with 1 associated CVE
› □ ●	Critical *	Vulnerable openbsd openssh with 1 associated CVE

CVEs as Risks Use Cases & Workflows

The following scenarios and flows illustrate just some of the many ways CVEs as Risks can be leveraged in practice.

Scenario	Workflow
Vulnerability Monitoring and Remediation User receives an alert highlighting new high-risk vulnerabilities in the attack surface.	1 Navigate to the "Risk Instances" page. 2 Identify a critical software vulnerability associated with multiple CVEs. 3 Review CVSS, KEV, and EPSS scores to assess the urgency of remediation. 4 Open a Jira ticket to prioritize remediation.
Investigating Critical CVEs A specific vulnerability is flagged by management for immediate investigation.	1 Search for the specific CVE in "Configure CVEs." 2 Identify impacted assets. 3 Research remediation steps via NVD links. 4 Plan and execute remediation while keeping management informed.
Filtering for the Right Volume of CVEs Large numbers of CVEs require proper filtering and tuning for effective management.	1 Adjust filters on the "Configure CVEs" page to prioritize higher-risk vulnerabilities. 2 Reduce the number of actionable CVEs to a manageable level.

Get Started Today

Maximize your vulnerability discovery and prioritization with the **CVEs as Risks in Censys ASM**. Speak to your CSM to learn how to integrate this capability into your workflow and stay ahead of emerging threats.

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.