

[← Blog](#)

Detect and prioritize CISA Known Exploited Vulnerabilities in the cloud with Wiz

For each CVE, the Wiz Research team maintains data from multiple threat intelligence sources and our own independent research. Now that we've added support for the new CISA KEV catalog, learn how you can use it in your cloud environment.



Alon Schindel

February 10, 2022

3 minute read



Table of contents

[What is the CISA KEV Catalog?](#)[Coverage for CISA KEV Catalog in Wiz](#)[Finding exploitable resources that pose the highest risk](#)[Risk-oriented vulnerability management](#)

Wiz supports the new **CISA Known Exploited Vulnerabilities (KEV) Catalog** as a source of exploit intelligence to vulnerability findings, on top of other sources. The new CISA binding directive helps enterprises to reduce cyber incidents by prioritizing the mitigation of vulnerabilities known to be actively exploited in order to improve the vulnerability management process. Vulnerabilities listed in the KEV catalog are less than 1% of the vulnerability findings in the cloud. Combined with the unique capabilities offered by Wiz to discover the toxic combinations that represent a real threat in your cloud environment, you can now better prioritize and focus on the risks that matter the most.

What is the CISA KEV Catalog?

CISA, the Cybersecurity & Infrastructure Security Agency, released a **binding operational directive** to reduce the significant risk of known exploited vulnerabilities. In recognition that vulnerabilities that have been previously exploited are a frequent vector for malicious cyber actors, CISA prioritizes these vulnerabilities as the biggest threats that must be aggressively remediated. Since November 2021, CISA has managed a catalog of known exploited

Orca Security Ltd.

Exhibit 2147

Wiz v. Orca

IPR2024-00863, -00864, -00865

Ex. 2147-001

actors, CISA prioritizes these vulnerabilities as the biggest threats that must be aggressively remediated. Since November 2021, CISA has managed a catalog of known exploited vulnerabilities that carry significant risk, along with remediation requirements. Federal agencies are compelled to patch these vulnerabilities within the timeframe defined by CISA.

Currently, there are more than 352 vulnerabilities in the [catalog](#), covering vulnerabilities in operating systems (e.g. Windows, Linux), proprietary applications (e.g. SolarWinds products, Zoho ManageEngine ServiceDesk), and open source projects (e.g. Apache HTTP Server, Log4j).

The [latest vulnerability](#), a Microsoft Win32k privilege escalation vulnerability (CVE-2022-21882), was added on February 4th, 2022 and required remediation action within 14 days. Even though the CISA directive is binding for US federal agencies specifically, it is quickly becoming a best security practice for public and private sectors as well.

Table of contents

What is the CISA KEV Catalog?

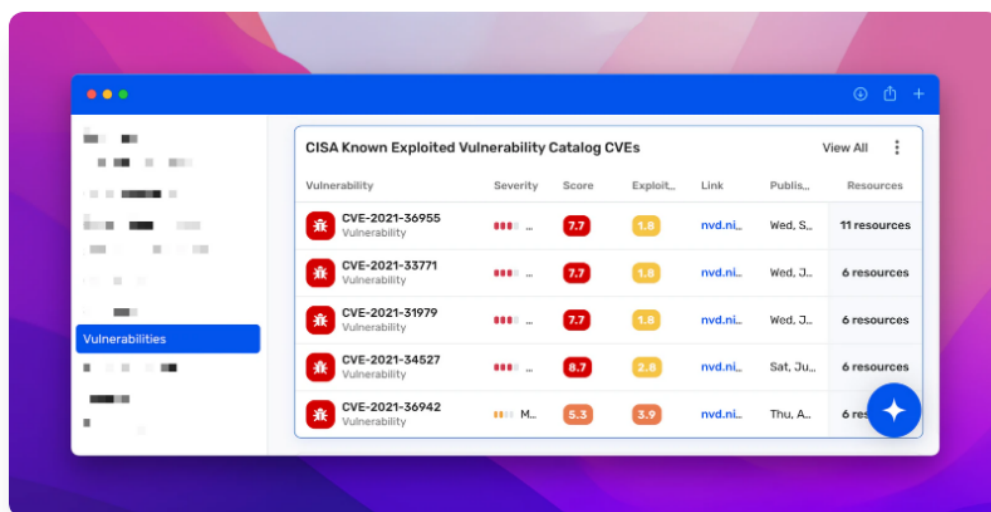
Coverage for CISA KEV Catalog in Wiz

Finding exploitable resources that pose the highest risk

Risk-oriented vulnerability management

Coverage for CISA KEV Catalog in Wiz

Wiz utilizes [agentless scanning](#) to build an inventory of your cloud infrastructure — across workloads, accounts, and environments. It delivers unified coverage across clouds and compute architectures from virtual machines and containers to serverless functions.



CISA Known Exploit Vulnerabilities Catalog CVEs dashboard in Wiz

For each CVE, the Wiz Research team maintains data from multiple threat intelligence sources and our own independent research. Now that we've added support for the new CISA KEV catalog, here's how you can use it in your cloud environment:

- Review the dedicated dashboard— You can immediately assess the vulnerability posture across your organization by logging into the new **CISA Known Exploited Vulnerability Catalog CVEs** dashboard, which lists all the resources in your cloud environment that are currently vulnerable to one or more vulnerabilities in the catalog.
- Use the dedicated search— You can query and locate all the VMs, containers, and serverless functions in your cloud environment that are vulnerable to a specific CVE in the catalog with a simple query shortcut.

catalog with a simple query shortcut.

Finding exploitable resources that pose the highest risk

Vulnerability management teams nowadays face hundreds or even thousands of vulnerabilities. It's quite challenging to try to remediate each one of them. So the question becomes, which ones should be prioritized?

Only less than 1% of the vulnerabilities that Wiz detects in the cloud are listed in the KEV catalog.

Wiz scans the entire stack to identify the toxic combinations that represent real risk to your environment. Using the Wiz contextual security graph, you can prioritize patching by focusing on these toxic combinations and finding the resources that pose the highest risk in your cloud environment. For example:

- Exposed resources— A vulnerable VM with access to the Internet poses a greater risk since it can be more easily exploited by malicious actors.
- High privileged resources— A vulnerable VM that can assume an admin IAM role or contains an API key with admin privileges is at much higher risk to gain control of your environment.

Leveraging the contextual understanding of your cloud environment provided by Wiz with the CISA KEV catalog input allows you to better prioritize and mitigate the critical risks in your environment, by locating your vulnerable assets that pose the highest risk. The example below shows a Wiz Security Graph view of a VM vulnerable to one or more vulnerabilities in the KEV Catalog, that also has access to the internet and private keys with highly privileged permissions. With such a combination of risk factors, this VM would represent a high priority asset to remediate.



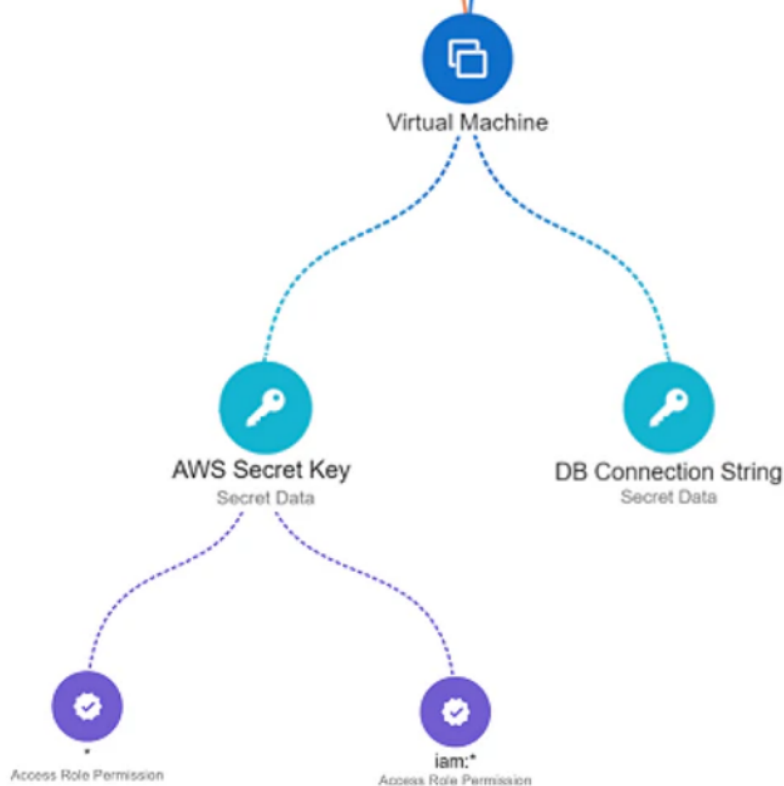
Table of contents

What is the CISA KEV Catalog?

Coverage for CISA KEV Catalog in Wiz

Finding exploitable resources that pose the highest risk

Risk-oriented vulnerability management



A vulnerable VM with internet access and private keys with highly privileged permissions on the Wiz Security Graph

Table of contents

What is the CISA KEV Catalog?

Coverage for CISA KEV Catalog in Wiz

Finding exploitable resources that pose the highest risk

Risk-oriented vulnerability management

Risk-oriented vulnerability management

The CISA KEV catalog is a valuable initiative that helps enterprises with their **vulnerability management** by which which vulnerabilities are known to be exploited. With the **agentless** patch management capabilities provided by Wiz and KEV insights combined, enterprises can identify and prioritize high impact vulnerabilities across their cloud environment to **significantly improve their security posture**.



Tags #Product

Continue reading

servicenow + wiz

Wiz and ServiceNow VR: Prioritize and respond to cloud vulnerabilities faster



Itay Arbel
March 1, 2022

Wiz is excited to announce its new integration with ServiceNow Vulnerability Response (VR), creating a combined...

"Positioning the security function as a business enabler is **critical**. To do this, you need to align the strategic goals of the security function with those of the board."



CLOUDSEC360

Five ways to bolster security as cloud environments and budgets come under attack



Wiz Team
April 13, 2023

Security experts share their insights for securing cloud environments as the pace and scale of threats accelerates.

Cloud + Kubernetes = ❤️

WIZ

Wiz rapidly finds and removes risks across the container development lifecycle and entire cloud environment



Yinon Costica
October 24, 2022

New Wiz capabilities protect containerized applications by bringing deep cloud context and visibility to quickly identify and prioritiz...

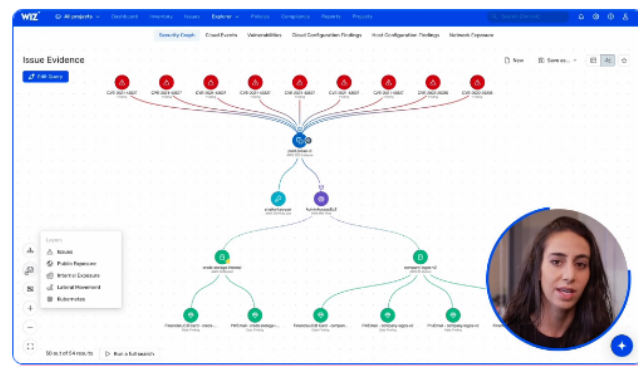
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

"Wiz provides a single pane of glass to see what is going on in our cloud environments."



Adam Fletcher
Chief Security Officer



Get a demo >



PLATFORM

Wiz CNAPP

Wiz Code

Wiz Cloud

Wiz Defend

Integrations

Environments

LEARN

Customer stories

Train Your Team For Cloud

Blog

CloudSec Academy

Resources Center

Cloud threat landscape

COMPANY

About Wiz

Join the team

Newsroom

Events

Contact us

Trust Center

English (US) ▾



