Vulnerability detection

From:
https://pandorafms.com/manual/!800/
Permanent link:
https://pandorafms.com/manual/!800/en/documentation/pandorafms/cybersecurity/30_vulnerabilities
2026/04/20 09:18

Vulnerability detection

Vulnerability Monitoring

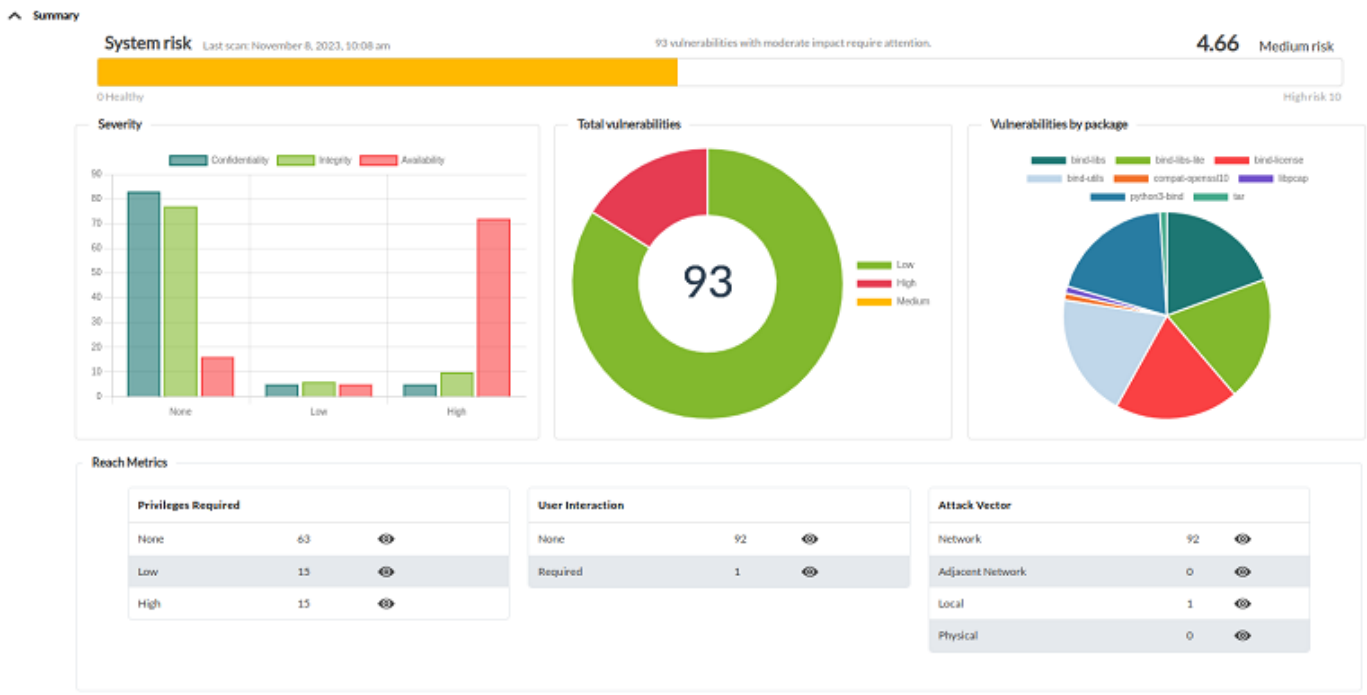
In a similar way to how the hardening evaluation is carried out, Pandora FMS EndPoints and the remote discovery engine will search for information about the software installed on the system, then compare this information with the central database of vulnerabilities that Pandora FMS has (downloaded from NIST, Miter and other sources) and will provide a list of software packages with known vulnerabilities.

This feature is available whether you have EndPoints (and these EndPoints have software inventory enabled) or if you do not have EndPoints and have to scan the network. If the network is scanned, the amount of information provided will be lower. It is recommended to use an agent.

Any version 7 EndPoint can be used for this as long as it has software inventory activated. This system works for Linux® and MS Windows® systems.

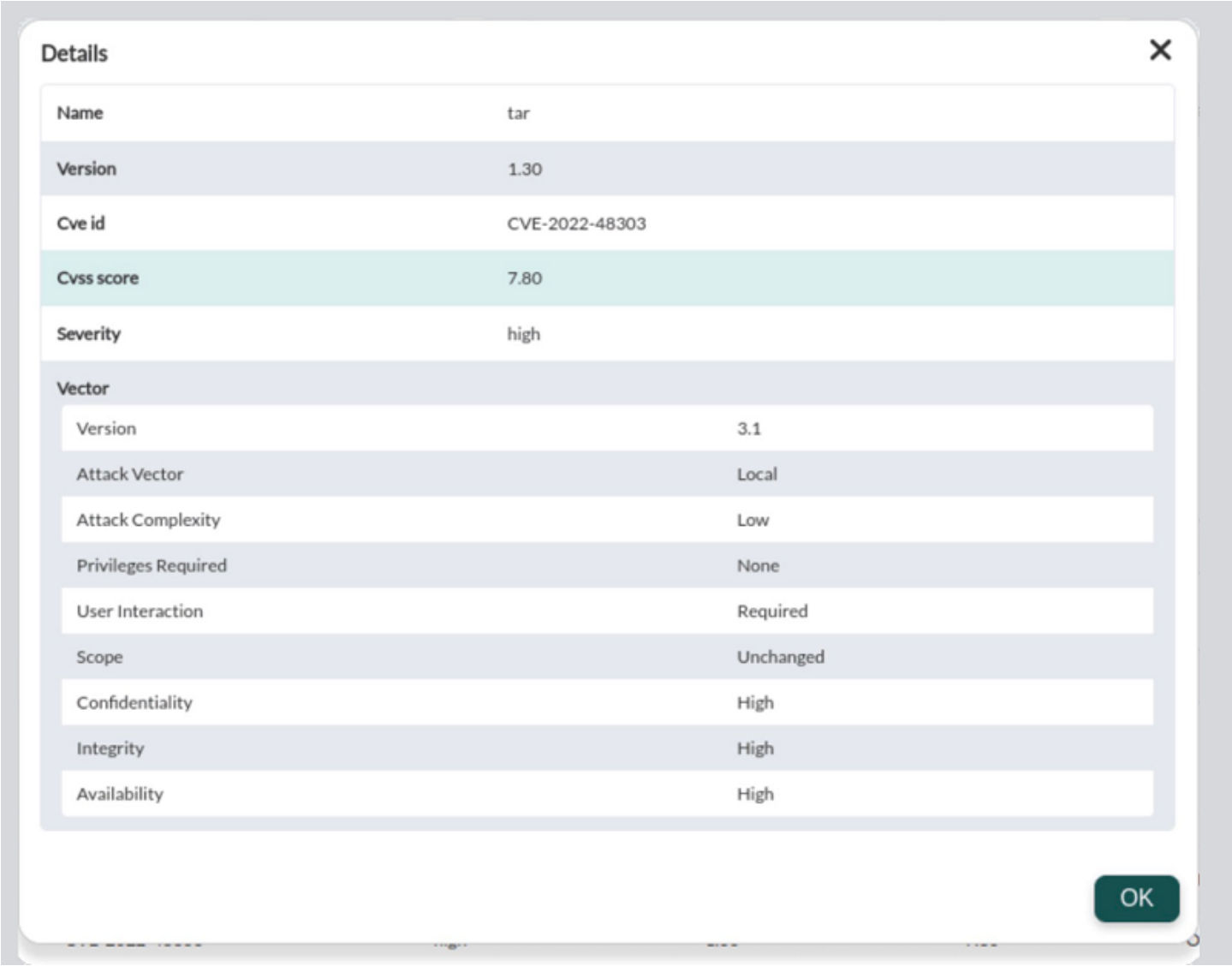
In a similar way to how hardening works, Pandora FMS will offer a unique risk indicator for each system, based on the number of vulnerabilities and their dangerousness.

It will provide an information panel of the system's vulnerabilities, indicating the evolution of the risk over time, the vulnerabilities sorted by different criteria, such as complexity of the attack, severity, type of vulnerability, attack vector, user interaction, type of privileges required, etc.



You may navigate through the control panel to filter the information and reach a level of detail where each vulnerable software package is specified, the vulnerability (with CVE code) that applies to it and the description of the problem:

Name	CVE	Severity	Version	Score	Detection Time	Details
tar	CVE-2022-48303	high	1.30	7.80	October 16, 2023, 8:55 am	
python3-bind	CVE-2022-38177	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2022-38178	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2021-25219	low	9.11.36	5.30	October 16, 2023, 8:55 am	
python3-bind	CVE-2021-25215	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8625	high	9.11.36	8.10	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8623	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8616	low	9.11.36	8.60	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8617	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6477	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6465	low	9.11.36	3.70	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6471	low	9.11.36	5.90	October 16, 2023, 8:55 am	
python3-bind	CVE-2018-5743	low	9.11.36	8.60	October 16, 2023, 8:55 am	
libpcap	CVE-2019-15165	low	1.9.1	7.50	October 16, 2023, 8:55 am	
compat-openssl10	CVE-2022-0778	low	1.0.2o	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2022-38177	low	9.11.36	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2022-38178	low	9.11.36	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2021-25219	low	9.11.36	5.30	October 16, 2023, 8:55 am	
bind-utils	CVE-2021-25215	low	9.11.36	7.50	October 16, 2023, 8:55 am	



What is a CVE?

Common Vulnerabilities and Exposures (CVE) is a unique, standardized identification for a security vulnerability in software or hardware. CVE are a naming and tracking system used around the world to identify and list specific security vulnerabilities. This system was created to make vulnerability information organization, communication and reference easier, allowing the cybersecurity community and IT professionals to address and solve security issues more efficiently.

The key features of a CVE are the following:

- Unique identification: Each CVE has a unique number that identifies it, making it easy to track and reference. For example, a CVE may have a format like “CVE-2021-12345.”
- Detailed Description: Each CVE includes a detailed description of the vulnerability, allowing users to better understand the nature and impact of the issue.
- Cross-references: CVEs often include cross-references to other security resources and databases, such as the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), to provide additional information about the vulnerability.

- Publication Date: CVEs normally include the date the vulnerability information was published.

CVEs are used by the computer security industry, software and hardware vendors, security researchers and system administrators to track and manage vulnerabilities. This standardized nomenclature is essential to ensure that vulnerabilities are communicated and addressed consistently around the world, helping to protect organizations and end users from security threats. Additionally, the existence of CVE makes it easier to create databases and tools that allow organizations to stay up to date with the latest threats and apply patches or security solutions when necessary.

The Pandora FMS vulnerabilities database

The Pandora FMS vulnerability database draws from two sources:

- CVE-Search which combines data from NVD NIST, MITER and Red Hat.
- Direct information from the repositories of Canonical, Red Hat, Debian, Arch Linux, NVD NIST, and Microsoft Security Updates.

The Pandora server builds its own database from this data and segments and indexes it in memory for quick detection, so that it only loads the vulnerabilities corresponding to the operating systems reported by Pandora FMS EndPoints.

To detect vulnerabilities using EndPoints, a database is used that is distributed by default with the PFMS server and associates package and application names with different CVEs. To detect remote vulnerabilities, a database is used that associates CPEs with CVEs. The console uses a database with information about the different CVEs found in the server database to display it to the user and generate reports. The data of the different CVEs are loaded in `tpandora_cve` table, which has existed since version 774.

Vulnerability Audit Configuration

At the server level

For local vulnerability detection, the Data Server must be activated and the EndPoints must send inventory information software.

For remote vulnerability detection to work the Discovery Server must be activated.

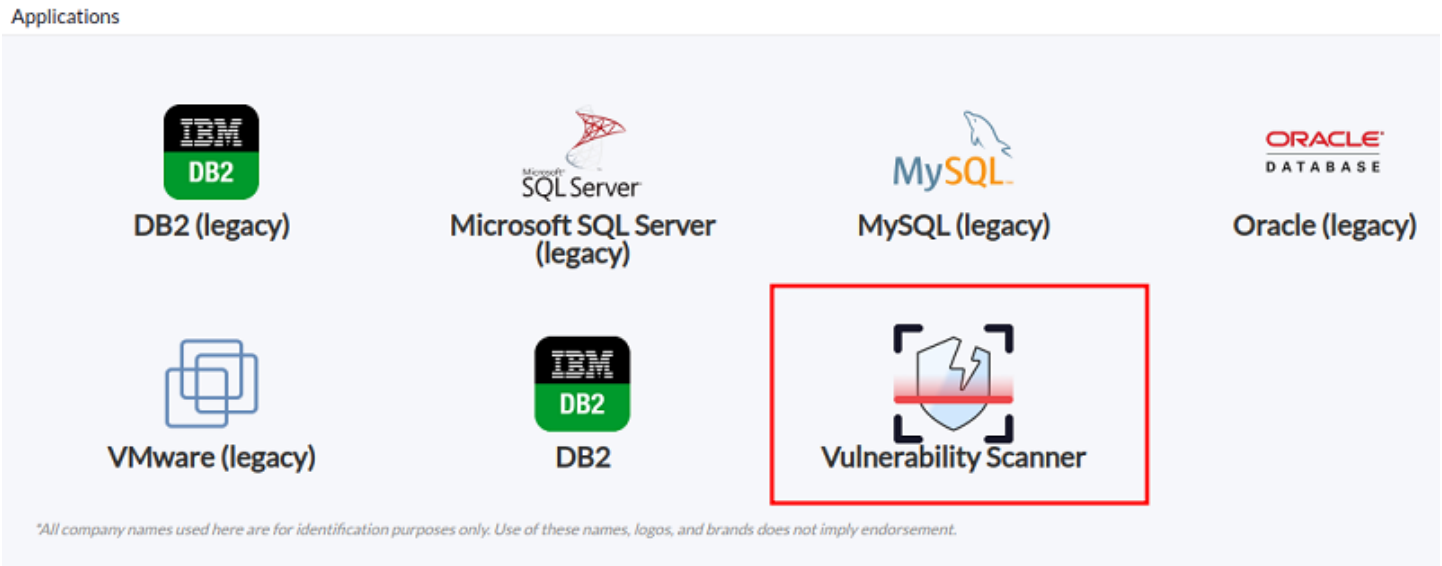
At agent level

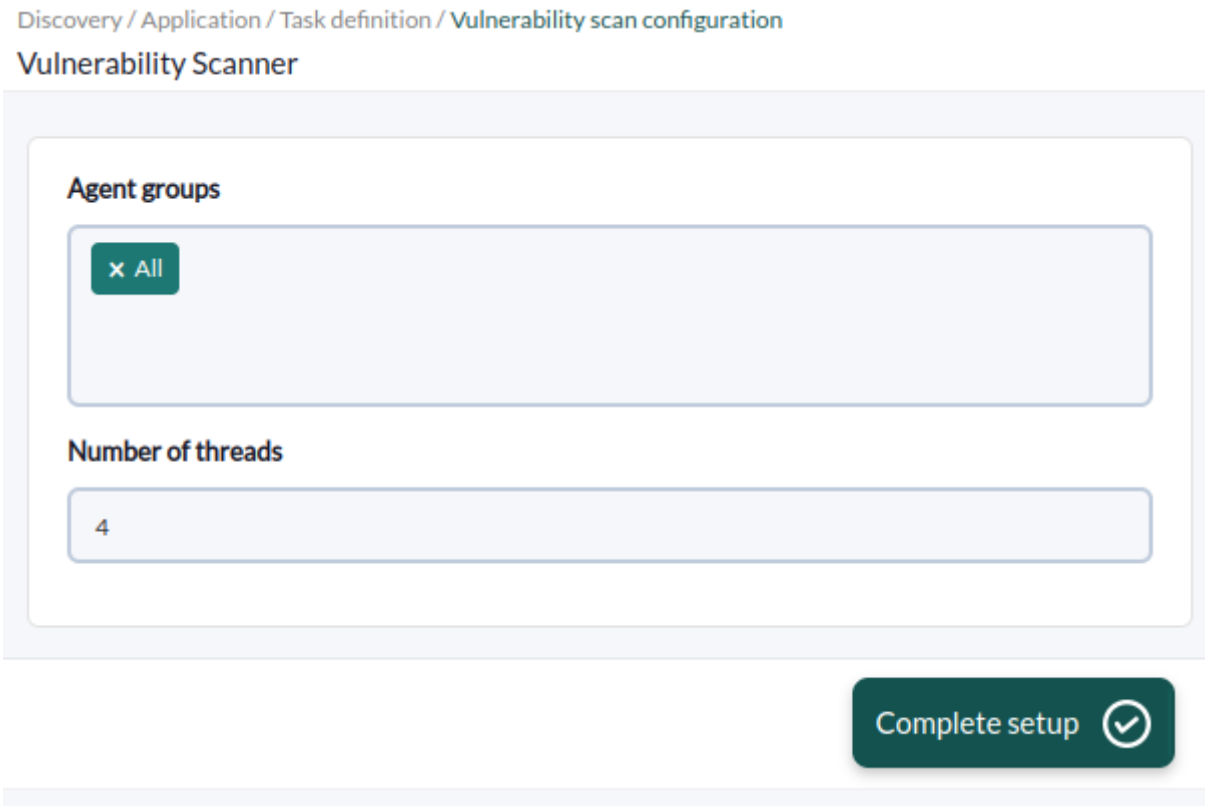
You may manually disable or enable agents, or have them use (by default) the global settings in the advanced settings section.

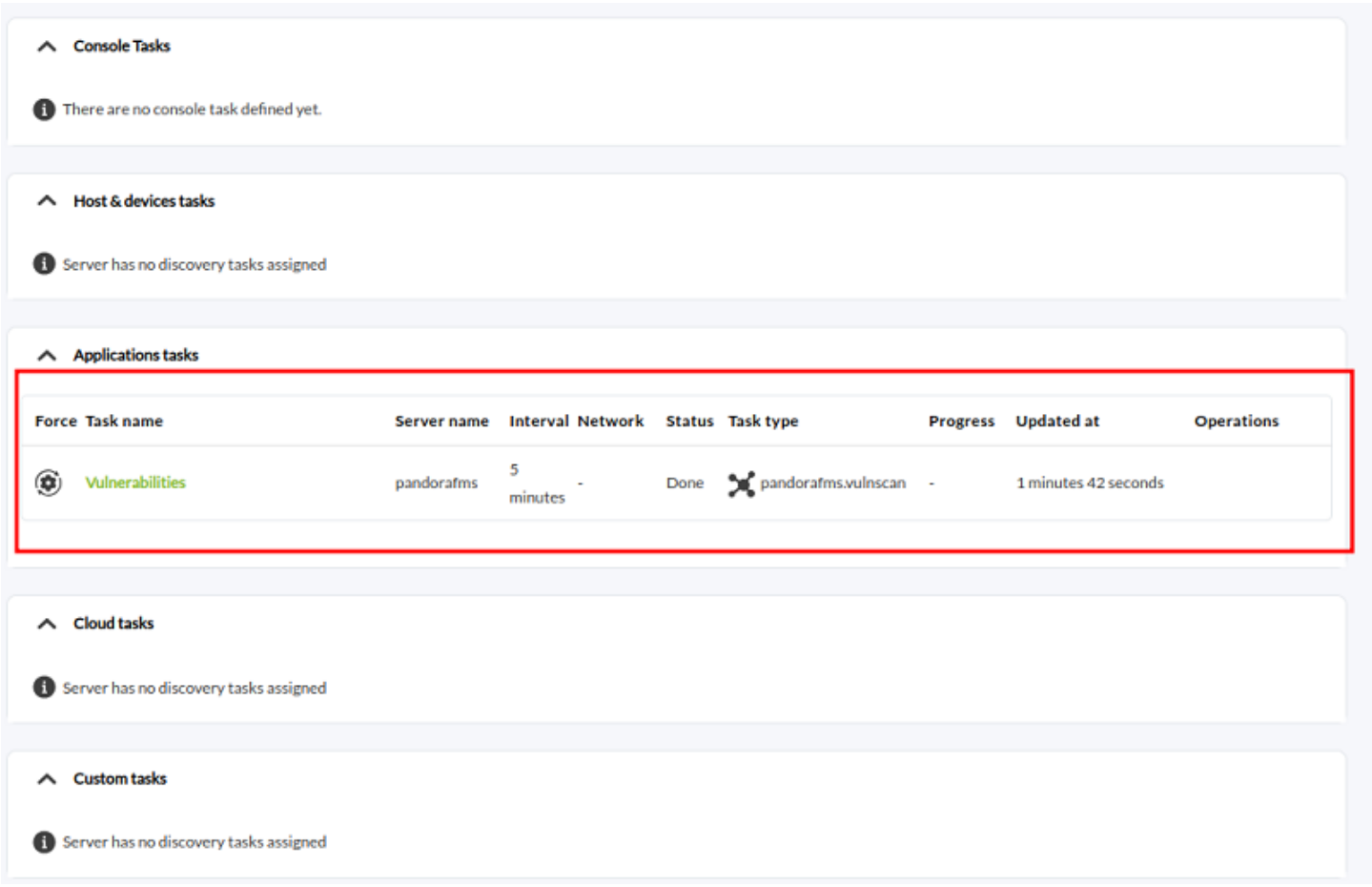
Remote Scan Tasks

To do this you must go to Discovery and launch a new vulnerability discovery task. You will be asked for one or more groups of machines that already exist in monitoring to launch vulnerability detection on them. The main IP address of these agents will be used to launch the scan. If you do not have monitoring or they do not exist in Pandora FMS, they must be detected first with a normal discovery network detection.

Vulnerability scanning will not create new agents.




Discovery / Application / Task definition / Vulnerability scan configuration
Vulnerability Scanner
Agent groups
× All
Number of threads
4
Complete setup


Console Tasks
There are no console task defined yet.
Host & devices tasks
Server has no discovery tasks assigned
Applications tasks
Force Task name Server name Interval Network Status Task type Progress Updated at Operations
Vulnerabilities pandorafms 5 minutes - Done pandorafms.vulnscan - 1 minutes 42 seconds
Cloud tasks
Server has no discovery tasks assigned
Custom tasks
Server has no discovery tasks assigned

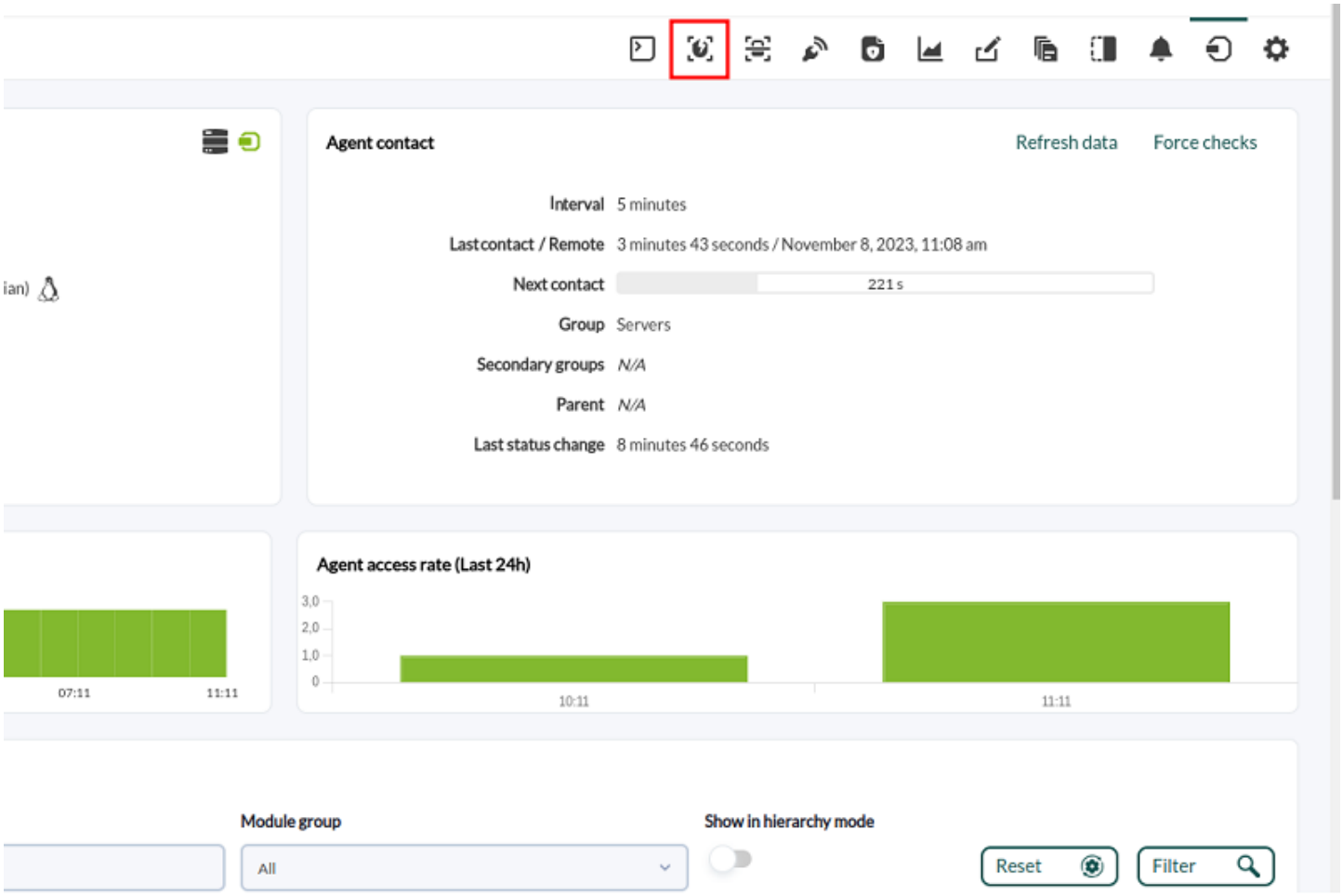
Vulnerability data display

Once the system has information, it will be displayed in the Vulnerabilities tab of each monitored system.

It also has (as of version 775) a general dashboard, with several added graphs, such as the Top-10 of most vulnerable systems (worst ranking of vulnerabilities), Top-10 vulnerabilities (most frequent) and other groupings.

These reports have some specific filters:

- By group of machines.
- Attack complexity (low/high/medium).
- Type of vulnerability (confidentiality, integrity, availability...).
- Access vector: Network, Adjacent Network...
- User interaction: none, required, etc.
- Privileges required: None, low...



Summary

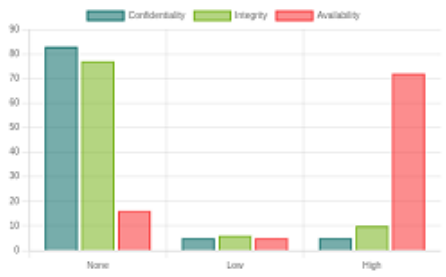
System risk Last scan: November 8, 2023, 11:23 am

93 vulnerabilities with moderate impact require attention.

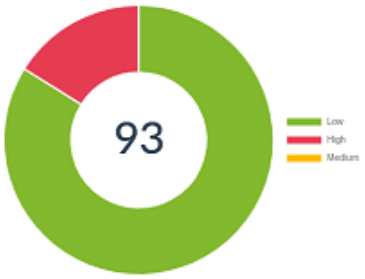
4.66 Medium risk

0 Healthy High risk 10

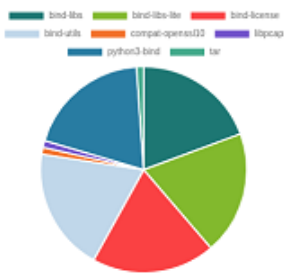
Severity



Total vulnerabilities



Vulnerabilities by package



Reach Metrics

Privileges Required		
None	63	
Low	15	
High	15	

User Interaction		
None	92	
Required	1	

Attack Vector		
Network	92	
Adjacent Network	0	
Local	1	
Physical	0	

Audit

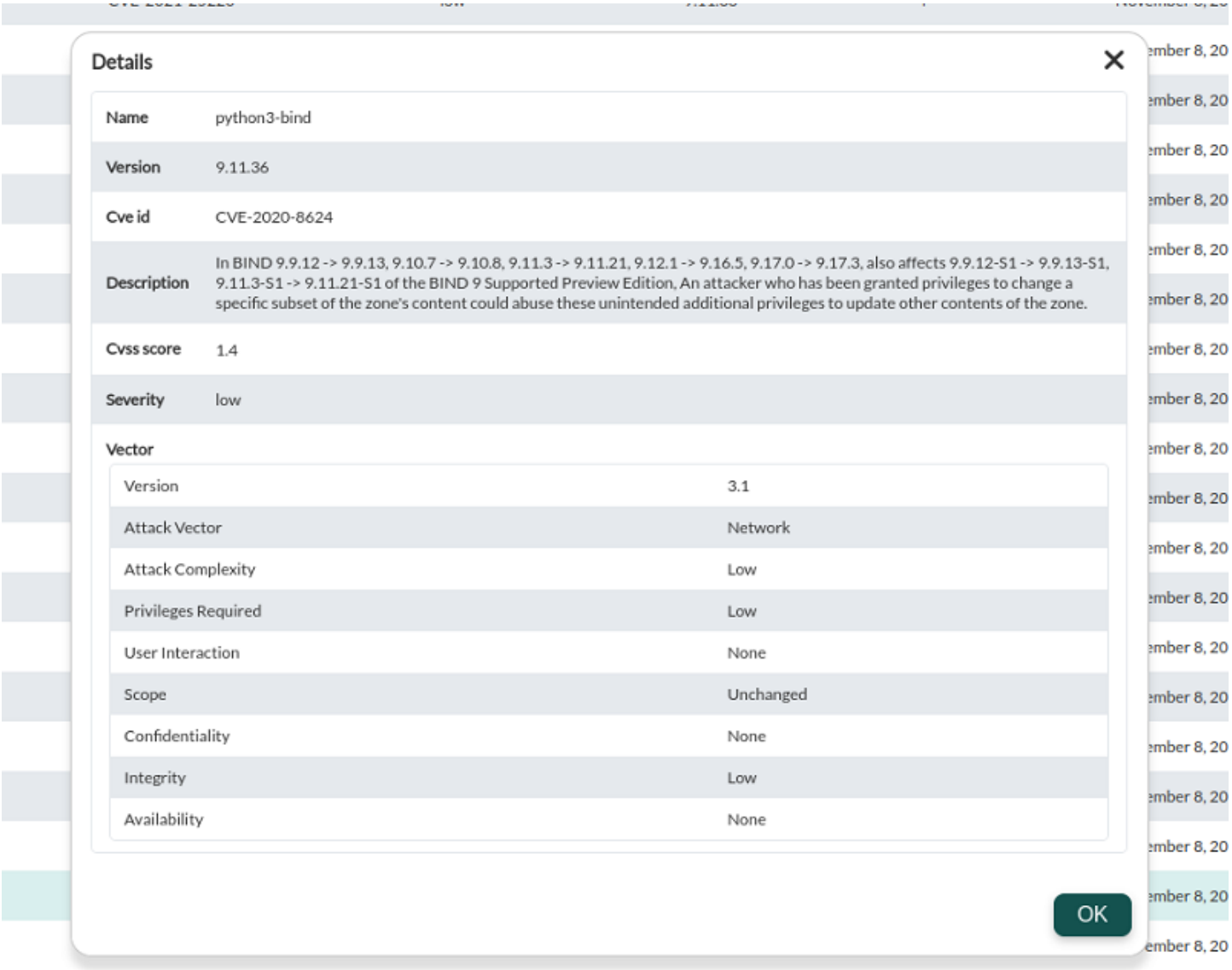
Filters

Detection Time: Last detection | Package: All | Severity: All | Attack Complexity: All | Privileges Required: All | User Interaction: All | Attack Vector: All

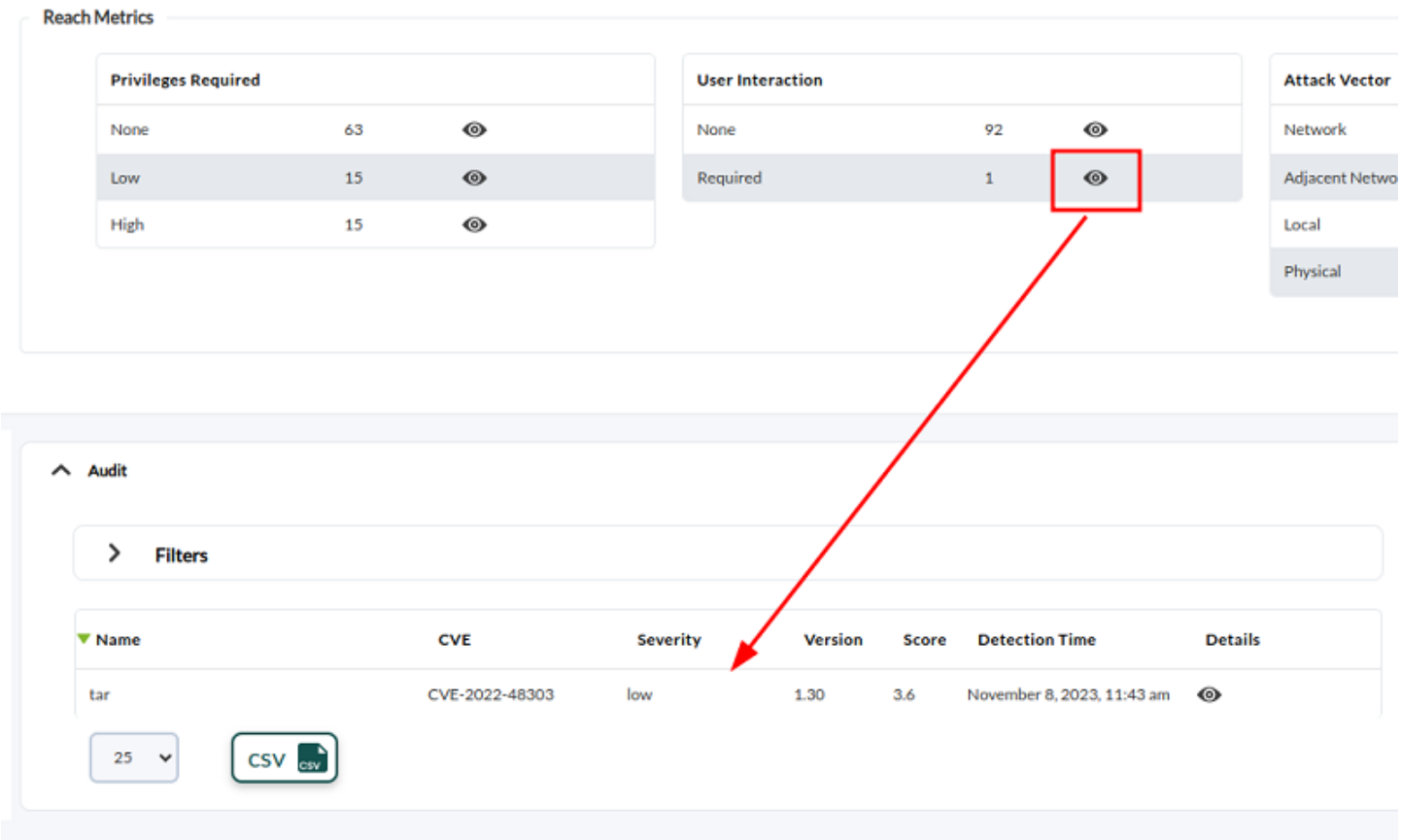
CVE

Filter

Name	CVE	Severity	Version	Score	Detection Time	Details
tar	CVE-2022-48303	low	1.30	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25220	low	9.11.36	4	November 8, 2023, 11:23 am	
python3-bind	CVE-2022-38177	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2022-38178	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25219	low	9.11.36	1.4	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25214	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25215	low	9.11.36	3.6	November 8, 2023, 11:23 am	



Scope metrics allow you to quickly filter out vulnerabilities:

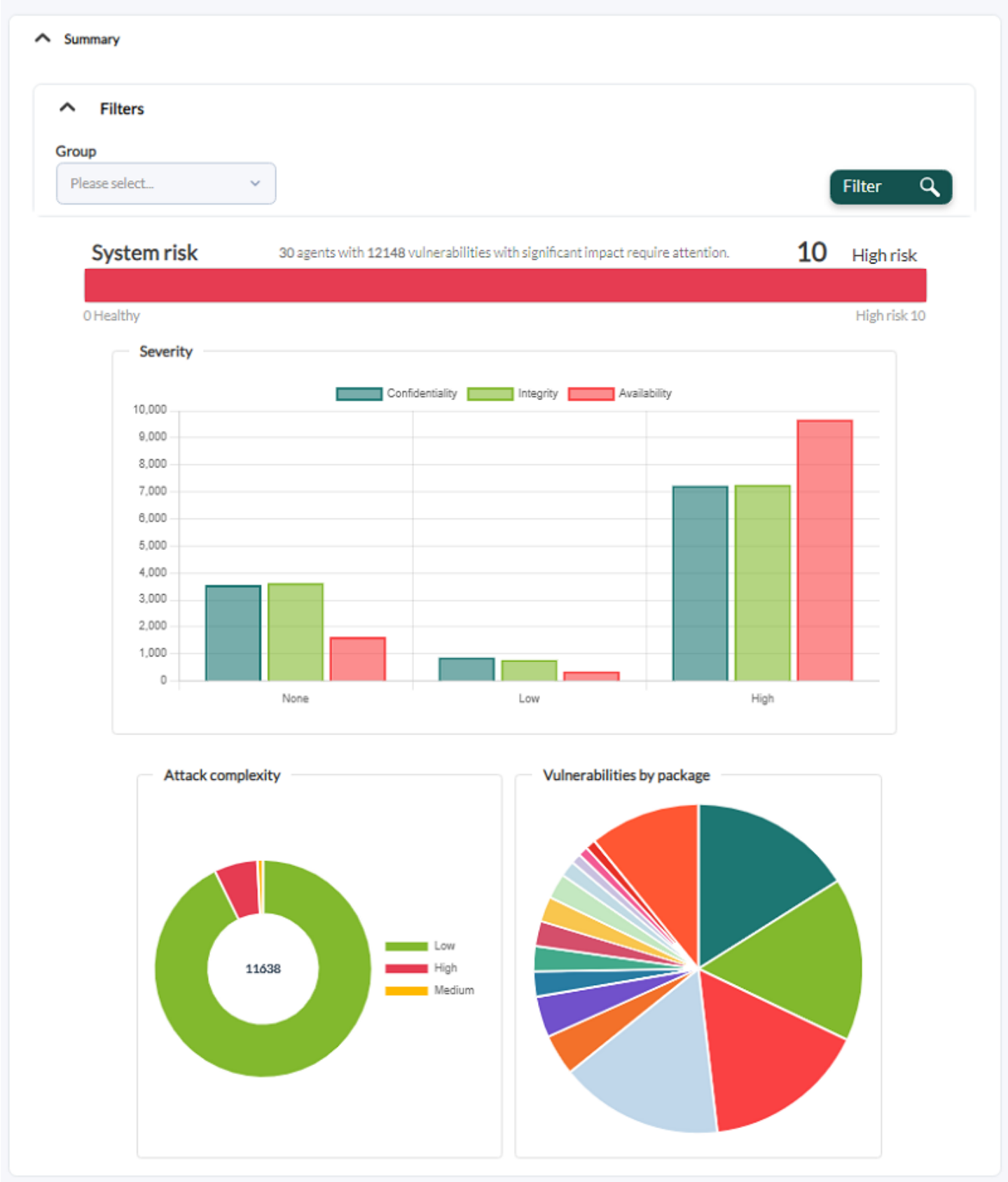


Tactical security view

Operation → Security → Vulnerabilities menu.

Summary

It presents an overall picture of the agents, with graphs summarizing the total system risk as a whole, the severity of the complexity of the attacks and the vulnerabilities presented by each installed software package.

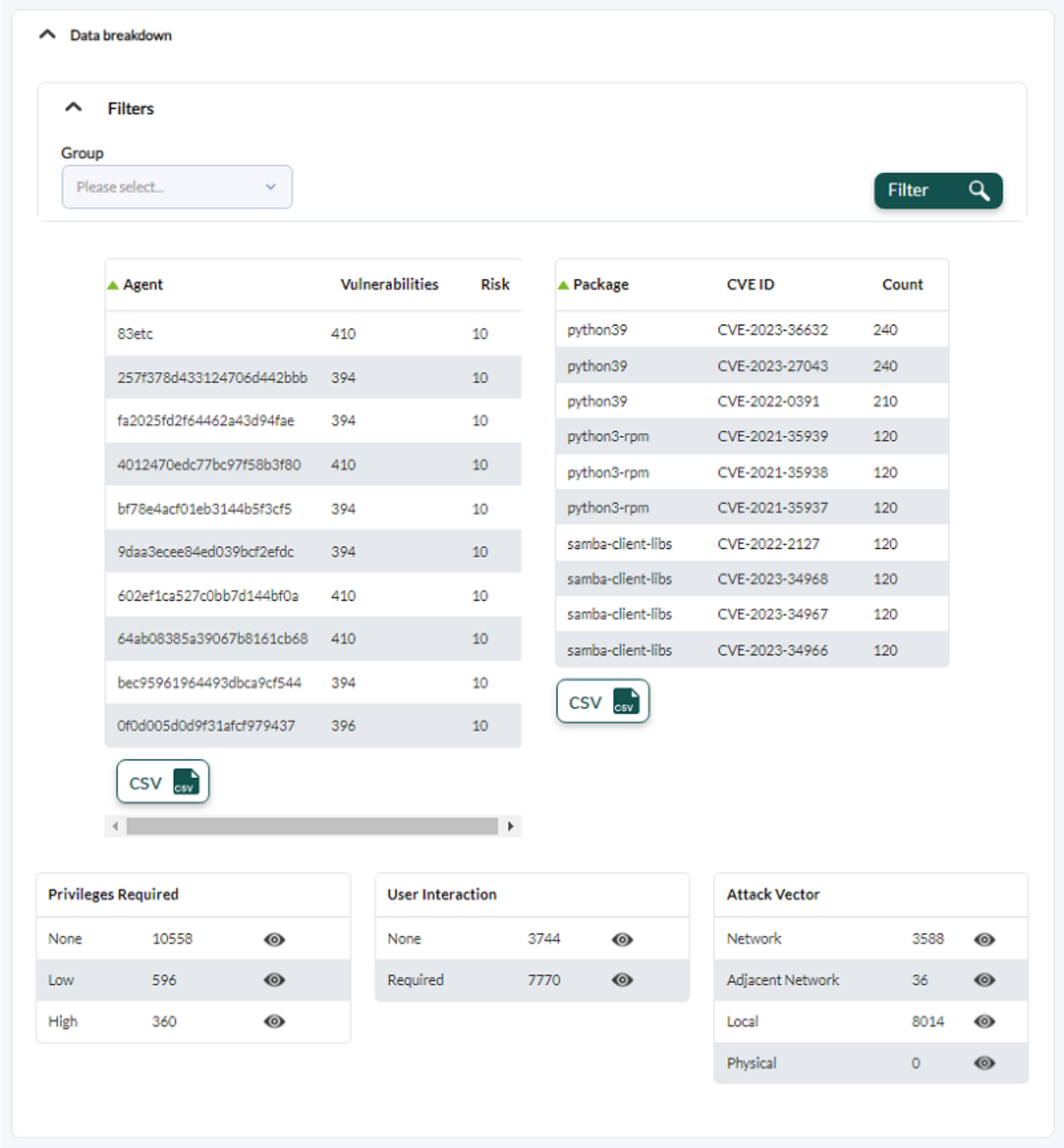


You may filter by agent group, all groups are displayed by default (All).

Data breakdown

It presents a breakdown of security data, showing the top 10 agents and top 10 software packages

with the most vulnerabilities.



Information can be filtered by agent groups and exported in CSV format. Summaries in Privileges required, User Interaction and Attack Vector boxes have display buttons that refer to the audit section.

Audit

By default it displays all vulnerability information, so it may take some time to load. You will be able to filter by infinite combinations of vulnerability features, including specific CVE identifier numbers.

Audit

Filters

Agent: All | Package: All | Severity: All | Attack Complexity: All

Privileges Required: All | User Interaction: All | Attack Vector: All

CVE:

Filter

Agent	Name	CVE	Severity	Version	Score	Detection Time	Details
fa2025fd2f64462a43d94fae	python39	CVE-2007-4559	low	3.9.7	6.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-32681	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-40217	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-24329	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2020-10735	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-45061	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2021-28861	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-42919	high	3.9.7	5.9	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2015-20107	low	3.9.7	4.7	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-36632	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-27043	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-0391	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2007-4559	low	3.9.7	6.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-32681	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-40217	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-24329	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2020-10735	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-45061	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2021-28861	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-42919	high	3.9.7	5.9	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2015-20107	low	3.9.7	4.7	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-36632	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-27043	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-0391	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-pip	CVE-2023-36632	low	20.7.4	3.6	December 7, 2023, 12:00 am	

Show 25 entries CSV

Previous 1 2 3 4 5 ... 486 Next

Once the information has been filtered, each item has a detail display button (eye icon) that will display the corresponding detailed information.

Return to Pandora FMS documentation index