



# Détection des vulnérabilités



From:

<https://pandorafms.com/manual/!803/>

Permanent link:

[https://pandorafms.com/manual/!803/fr/documentation/pandorafms/cybersecurity/30\\_vulnerabilities](https://pandorafms.com/manual/!803/fr/documentation/pandorafms/cybersecurity/30_vulnerabilities)

2026/08/31 14:15



# Détection des vulnérabilités

## Supervision des vulnérabilités

De la même manière que l'évaluation du renforcement est effectuée, les agents Pandora FMS et le moteur de découverte à distance rechercheront des informations sur les logiciels installés sur le système, puis compareront ces informations avec la base de données centrale de vulnérabilités de Pandora FMS (téléchargée depuis NIST, Mitre et autres sources) et fournira une liste de logiciels présentant des vulnérabilités connues.

Cette fonctionnalité est disponible que vous disposiez d'EndPoints (et que l'inventaire logiciel soit activé sur ces agents) ou si vous n'avez pas d'agents et devez effectuer une découverte sur le réseau. Si la découverte se fait via le réseau, les informations fournies seront bien moindres. Il est recommandé d'utiliser un agent.

N'importe quel agent version 7 peut être utilisé pour cela à condition que son inventaire logiciel soit activé. Ce système fonctionne pour les systèmes Linux® et MS Windows®.

De la même manière que le renforcement, Pandora FMS proposera un indicateur de risque unique pour chaque système, basé sur le nombre de vulnérabilités et leur dangerosité.

Il fournira un panneau d'information sur les vulnérabilités du système, indiquant l'évolution du risque dans le temps, les vulnérabilités classées selon différents critères, tels que la complexité de l'attaque, la gravité, le type de vulnérabilité, le vecteur d'attaque, l'interaction de l'utilisateur, le type de privilèges requis, etc.

## Summary

## System risk

Last scan: November 8, 2023, 10:08 am

93 vulnerabilities with moderate impact require attention.

4.66

Medium risk

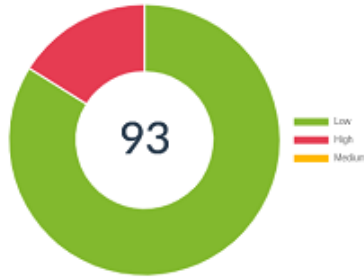
0 Healthy

High risk 10

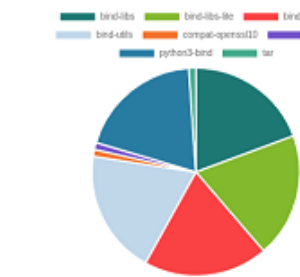
## Severity



## 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  | 👁 |

Vous pouvez naviguer dans le panneau de configuration pour filtrer les informations et atteindre un niveau de détail où est spécifié chaque progiciel vulnérable, la vulnérabilité (avec code CVE) qui s'y applique et la description du problème:



| ▼ 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 |         |

Details

Name

tar

Version

1.30

Cve id

CVE-2022-48303

Cvss score

7.80

Severity

high

Vector

Version

3.1

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

OK

## Qu'est-ce qu'un CVE ?

Les Common Vulnerabilities and Exposures (CVE) sont une identification unique et standardisée d'une vulnérabilité de sécurité logicielle ou matérielle. Les CVE sont un système de nommage et de suivi utilisé dans le monde entier pour identifier et répertorier des vulnérabilités de sécurité spécifiques. Ce système a été créé pour faciliter l'organisation, la communication et la référence des informations sur les vulnérabilités, permettant ainsi à la communauté de la cybersécurité et aux professionnels de l'informatique d'aborder et de résoudre les problèmes de sécurité plus efficacement.

Les principales caractéristiques d'un CVE sont les suivantes:

- Identification unique: Chaque CVE possède un numéro unique qui l'identifie, ce qui facilite son suivi et sa référence. Par exemple, un CVE peut avoir un format tel que « CVE-2021-12345 ».
- Description détaillée: Chaque CVE comprend une description détaillée de la vulnérabilité, permettant aux utilisateurs de mieux comprendre la nature et l'impact du problème.
- Références croisées: Les CVE incluent souvent des références croisées à d'autres ressources et bases de données de sécurité, telles que la Institut national des normes et de la technologie (NIST) National

Vulnerability Database (NVD), pour fournir des informations supplémentaires sur la vulnérabilité.

- Date de publication: Les CVE incluent généralement la date à laquelle les informations sur la vulnérabilité ont été publiées.

Les CVE sont utilisés par l'industrie de la sécurité informatique, les fournisseurs de logiciels et de matériel et les chercheurs en sécurité et les administrateurs système pour suivre et gérer les vulnérabilités. Cette nomenclature standardisée est essentielle pour garantir que les vulnérabilités sont communiquées et traitées de manière cohérente dans le monde entier, contribuant ainsi à protéger les organisations et les utilisateurs finaux contre les menaces de sécurité. De plus, l'existence de CVE facilite la création de bases de données et d'outils permettant aux organisations de se tenir au courant des dernières menaces et d'appliquer des correctifs ou des solutions de sécurité si nécessaire.

## La base de données des vulnérabilités Pandora FMS

La **base de données de vulnérabilités Pandora FMS** s'appuie sur deux sources:

- CVE-Search qui combine les données de NVD NIST, MITRE et Red Hat.
- Informations directes des référentiels de mises à jour de sécurité Canonical, Red Hat, Debian, Arch Linux, NVD NIST et Microsoft.

Le serveur Pandora construit sa propre base de données à partir de ces données, les segmente et les indexe en mémoire pour une détection rapide, afin de charger uniquement les vulnérabilités correspondant aux systèmes d'exploitation signalées par les agents Pandora FMS.

Pour détecter les vulnérabilités à l'aide d'agents, on utilise une base de données distribuée par défaut avec le serveur PFMS et qui associe les noms de packages et d'applications à différents CVE. Pour détecter les vulnérabilités à distance, une base de données est utilisée qui associe les CPE aux CVE. La console utilise une base de données contenant des informations sur les différents CVE trouvés dans la base de données du serveur pour les afficher à l'utilisateur et générer des rapports. Les données des différents CVE sont chargées dans la table `tpandora_cve`, qui existe depuis la version 774.

## Configuration de l'audit de vulnérabilité

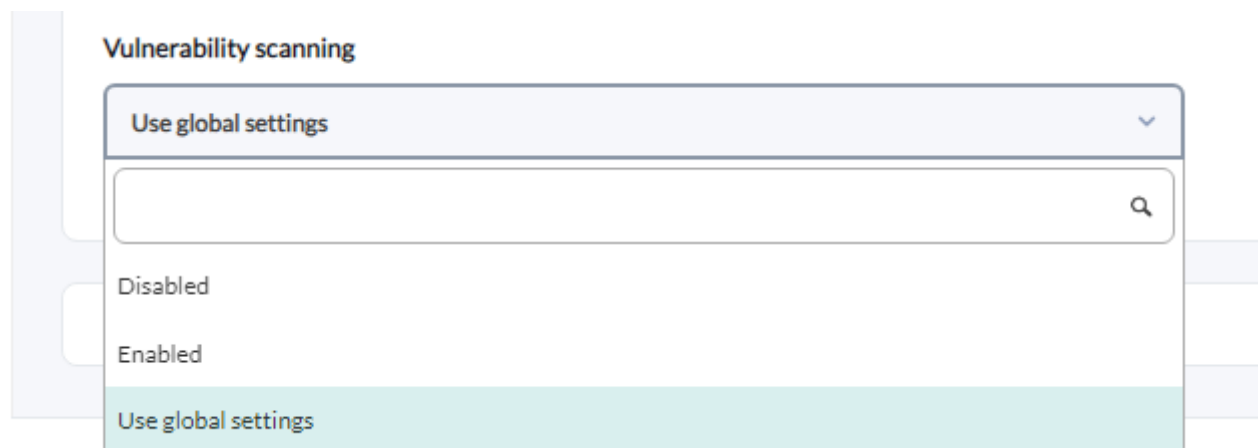
### Au niveau du serveur

Pour la détection locale des vulnérabilités, le **Data Server** doit être activé et les agents **doivent envoyer un logiciel d'informations d'inventaire**.

Pour que la détection des vulnérabilités à distance fonctionne, **le serveur Discovery doit être activé.**

## Au niveau de l'agent

Vous pouvez désactiver ou activer manuellement un agent ou utiliser (par défaut) la configuration globale du *setup*, dans la **section de configuration avancée**.



## Tâches d'analyse à distance

Pour ce faire, vous devez vous rendre sur **Discovery** et lancer une nouvelle tâche de découverte de vulnérabilité. Il vous sera demandé un ou plusieurs groupes de machines déjà existantes dans la supervision pour lancer la détection de vulnérabilités sur celles-ci. L'adresse IP principale de ces agents sera utilisée pour lancer le scan. Si vous n'avez pas de supervision ou s'ils n'existent pas dans Pandora FMS, ils doivent d'abord être détectés avec une détection de réseau de découverte normale.

L'analyse des vulnérabilités ne créera pas de nouveaux agents.



## Applications



DB2 (legacy)

Microsoft SQL Server  
(legacy)

MySQL (legacy)



Oracle (legacy)



VMware (legacy)



DB2



*\*All company names used here are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.*

Discovery / Application / Task definition / Vulnerability scan configuration

## Vulnerability Scanner

## Agent groups

x 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*

## Affichage des données de vulnérabilité

Une fois que le système dispose d'informations, celles-ci seront affichées dans l'onglet Vulnérabilités de chaque système supervisé.

Il dispose également (à partir de la version 775) d'un tableau de bord général, avec plusieurs graphiques ajoutés, comme le Top-10 des systèmes les plus vulnérables (pire classement des vulnérabilités), le Top-10 vulnerabilities (les plus fréquents) et autres regroupements.

Ces rapports comportent des filtres spécifiques:

- Par groupe de machines.
- Attack complexity (low/high/medium).
- Type de vulnérabilité (confidentiality, integrity, availability...).
- Access vector: Network, Adjacent Network...
- User interaction: none, required, etc.
- Privileges required: None, low...

[illegible]

**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**

| Category | Confidentiality | Integrity | Availability |
|----------|-----------------|-----------|--------------|
| None     | 82              | 78        | 16           |
| Low      | 4               | 5         | 4            |
| High     | 4               | 10        | 71           |

**Total vulnerabilities**

93

- Low
- High
- Medium

**Vulnerabilities by package**

- bind-libs
- bind-libs-libs
- bind-license
- bind-utils
- compat-openjdk
- libcap
- python3-bind
- tar

**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 |         |

**Details**

Name: python3-bind

Version: 9.11.36

Cve id: CVE-2020-8624

Description: In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone.

Cvss score: 1.4

Severity: low

**Vector**

|                     |           |
|---------------------|-----------|
| Version             | 3.1       |
| Attack Vector       | Network   |
| Attack Complexity   | Low       |
| Privileges Required | Low       |
| User Interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | None      |
| Integrity           | Low       |
| Availability        | None      |

OK

Les métriques de portée vous permettent de filtrer rapidement les vulnérabilités:

**Reach Metrics**

| Privileges Required |    |  |
|---------------------|----|--|
| None                | 63 |  |
| Low                 | 15 |  |
| High                | 15 |  |

| User Interaction |    |  |
|------------------|----|--|
| None             | 92 |  |
| Required         | 1  |  |

| Attack Vector  |
|----------------|
| Network        |
| Adjacent Netwo |
| Local          |
| Physical       |

**Audit**

> Filters

| Name | CVE            | Severity | Version | Score | Detection Time             | Details |
|------|----------------|----------|---------|-------|----------------------------|---------|
| tar  | CVE-2022-48303 | low      | 1.30    | 3.6   | November 8, 2023, 11:43 am |         |

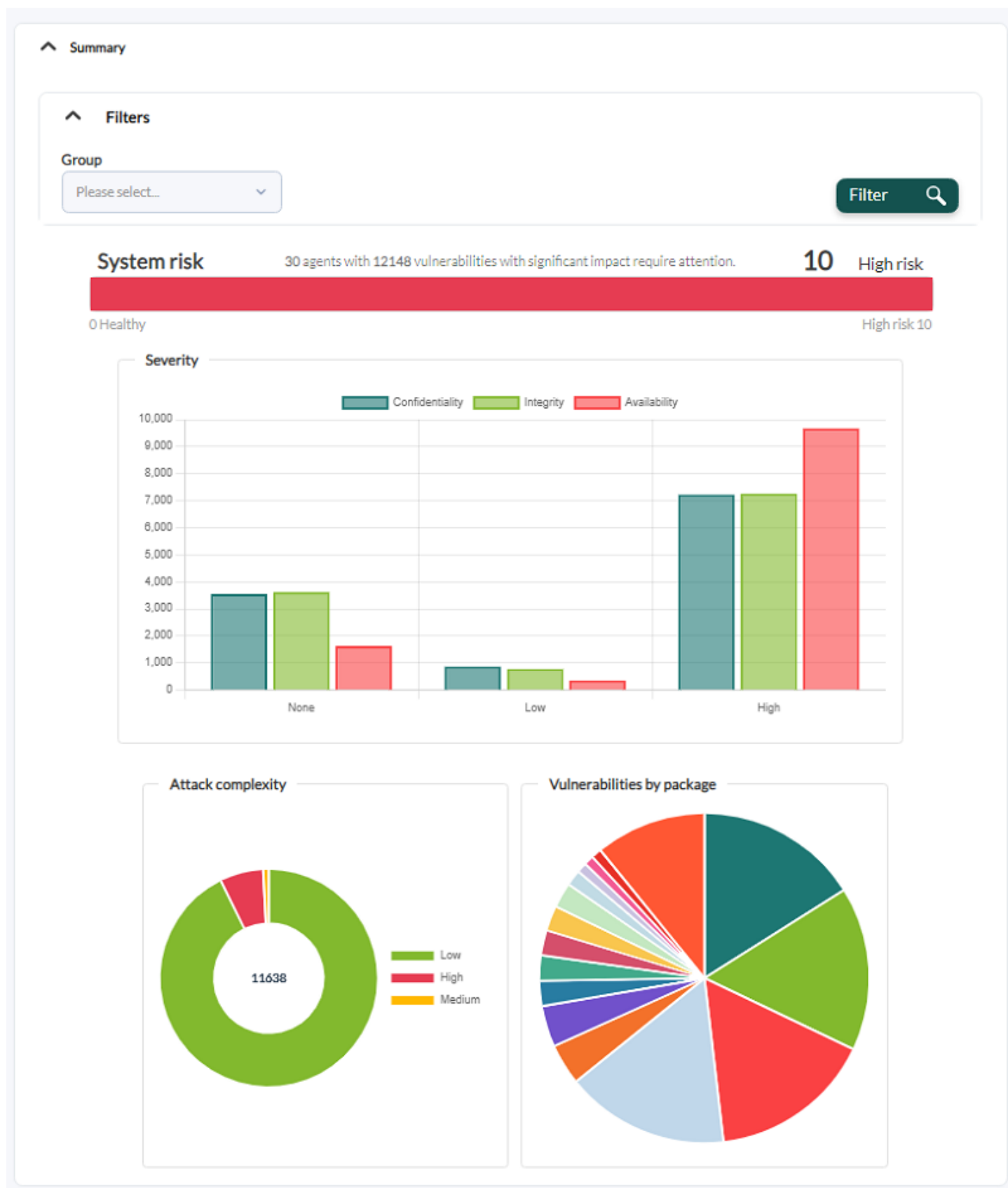
25

## Vision tactique de la sécurité

Menu Operation → Security → Vulnerabilities.

### Summary

Il présente une image globale des agents, avec des graphiques résumant le risque total dans le système dans son ensemble, la gravité de la complexité des attaques et les vulnérabilités présentées par chaque logiciel installé.



Vous pouvez filtrer par groupe d'agents; par défaut, tous les groupes sont affichés (All).

## Data breakdown

Il présente une ventilation des données relatives à la sécurité, en indiquant les 10 principaux

agents et les 10 principaux logiciels présentant le plus grand nombre de vulnérabilités.

Data breakdown

Filters

Group

Please select...

Filter

| Agent                    | Vulnerabilities | Risk |
|--------------------------|-----------------|------|
| 83etc                    | 410             | 10   |
| 257f378d433124706d442bbb | 394             | 10   |
| fa2025fd2f64462a43d94fae | 394             | 10   |
| 4012470edc77bc97f58b3f80 | 410             | 10   |
| bf78e4acf01eb3144b5f3cf5 | 394             | 10   |
| 9daa3ecee84ed039bcf2efdc | 394             | 10   |
| 602ef1ca527c0bb7d144bf0a | 410             | 10   |
| 64ab08385a39067b8161cb68 | 410             | 10   |
| bec95961964493dbca9cf544 | 394             | 10   |
| 0f0d005d0d9f31afcf979437 | 396             | 10   |

CSV

| Package           | CVE ID         | Count |
|-------------------|----------------|-------|
| python39          | CVE-2023-36632 | 240   |
| python39          | CVE-2023-27043 | 240   |
| python39          | CVE-2022-0391  | 210   |
| python3-rpm       | CVE-2021-35939 | 120   |
| python3-rpm       | CVE-2021-35938 | 120   |
| python3-rpm       | CVE-2021-35937 | 120   |
| samba-client-libs | CVE-2022-2127  | 120   |
| samba-client-libs | CVE-2023-34968 | 120   |
| samba-client-libs | CVE-2023-34967 | 120   |
| samba-client-libs | CVE-2023-34966 | 120   |

CSV

Privileges Required

|      |       |  |
|------|-------|--|
| None | 10558 |  |
| Low  | 596   |  |
| High | 360   |  |

User Interaction

|          |      |  |
|----------|------|--|
| None     | 3744 |  |
| Required | 7770 |  |

Attack Vector

|                  |      |  |
|------------------|------|--|
| Network          | 3588 |  |
| Adjacent Network | 36   |  |
| Local            | 8014 |  |
| Physical         | 0    |  |

Les informations peuvent être filtrées par groupe d'agents et exportées au format CSV. Les résumés dans les cases Privileges required, User Interaction et Attack Vector ont des boutons d'affichage qui renvoient à la section [audit](#).

## Audit

Par défaut, il affiche toutes les informations sur les vulnérabilités, ce qui peut prendre un certain temps de chargement. Vous pouvez filtrer par un nombre quelconque de combinaisons de caractéristiques de vulnérabilité, y compris des numéros d'identification CVE spécifiques.



## 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

Une fois les informations filtrées, chaque élément dispose d'un bouton d'affichage détaillé (icône en forme d'œil) qui permet d'afficher les informations détaillées correspondantes.

[Revenir à l'index de la documentation Pandora FMS](#)