



脆弱性検出



om:

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

ermanent link:

https://pandorafms.com/manual/!current/ja/documentation/pandorafms/cybersecurity/30_vulnerabilities

026/06/03 19:49



脆弱性検出

[Pandora FMS ドキュメント一覧に戻る](#)

脆弱性監視

強化評価の実行方法と同様に、Pandora FMS エンドポイントとリモート検出エンジンは、システムにインストールされたソフトウェアに関する情報を検索し、この情報を Pandora FMS が持つ脆弱性の中央データベース (NIST/Miter などのソースからダウンロード) と比較し、既知の脆弱性を持つソフトウェアパッケージのリストを提供します。

この機能は、エンドポイントがある場合 (およびこれらのエンドポイントでソフトウェアインベントリが有効になっている場合)、またはエンドポイントが存在せずネットワークをスキャンする必要がある場合に使用できます。ネットワークがスキャンされる場合、提供される情報量は少なくなります。エージェントを使用することをお勧めします。

ソフトウェアインベントリが有効である限り、バージョン7の全てのエンドポイントが使用できます。このシステムは Linux® と MS Windows® システムで動作します。

強化と同様の仕組みで Pandora FMS は脆弱性の数とその危険性に基づいた各システムごとのリスク指標を提供します。

これはシステム脆弱性の情報パネルを提供し、時間経過ごとのリスクの進化を示し、攻撃の複雑さ、重大度、脆弱性の種類、攻撃ベクトル、ユーザ操作、必要な権限の種類といった様々な基準で分類した脆弱性を表示します。

Summary

System risk

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

93 vulnerabilities with moderate impact require attention.

4.66 Medium risk

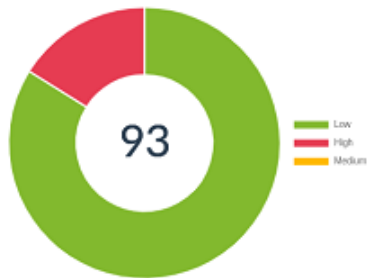
0 Healthy

High risk 10

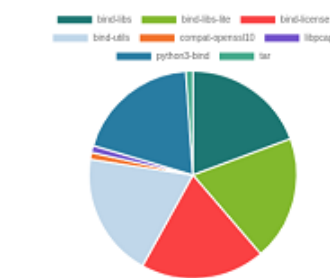
Severity



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 | 👁 |

コントロールパネルを操作して情報をフィルタし、脆弱なソフトウェアパッケージが指定された詳細レベルと、それに適用される脆弱性(CVE コード付き)と問題の説明を表示できます。

| ▼ 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 |

CVE とは?

CVE(Common Vulnerabilities and Exposures, 共通脆弱性識別子) はソフトウェアやハードウェアのセキュリティ脆弱性に対するユニークで標準化された識別子です。CVE は特定のセキュリティ脆弱性を識別しリスト化するため世界中で利用されている命名 追跡システムです。このシステムは脆弱性情報の整理、伝達、参照を容易にし、サイバーセキュリティコミュニティと IT プロフェッショナルがセキュリティの問題により効率的に対処して解決できるようにするため作成されました。

CVEの鍵となる特徴は以下です。

- 固有識別: 各 CVE は識別のための固有の番号を持ち、追跡や参照を容易にします。例えば [CVE-2021-12345] のようなフォーマットになります。
- 詳細な説明: 各 CVE は脆弱性の詳細な説明を含んでおり、ユーザが問題の性質と影響をより良く理解できます。
- 相互参照: CVE はしばしば米国国立標準技術研究所(NIST)の国家脆弱性データベース(NVD)といった他のセキュリティリソースやデータベースとの相互参照を含んでおり、脆弱性についての追加情報を提供しています。
- 発行日: CVE は通常脆弱性情報が公開された日付を含んでいます。

CVE はコンピュータセキュリティ産業、ソフトウェア・ハードウェアベンダー、セキュリティ研究者、システム管理者が脆弱性を追跡し管理するために利用されています。この標準化された命名法は脆弱性を世界中に一貫して伝達 対処し、組織とエンドユーザをセキュリティの脅威から保護するのに不可欠です。加えて CVE の存在は、組織が最新の脅威を把握し、必要に応じパッチ適用やセキュリティ対策を取るためのデータベースやツールを作成することを容易にします。

Pandora FMS 脆弱性データベース

Pandora FMS 脆弱性データベースは2つのソースから取得されます。

- NVD NIST、MITER、Red Hat からデータを組み合わせた CVE 検索
- Canonical、Red Hat、Debian、Arch Linux、NVD NIST、Microsoft Security Updates のリポジトリからの直接情報

Pandora サーバーはこのデータから独自のデータベースを構築し、メモリ内でセグメント化とインデックス作成を行い迅速な検出を実現します。これにより Pandora FMS エンドポイントによって報告されたオペレーティングシステムに対応する脆弱性のみが読み込まれます。

エンドポイントを用いて脆弱性を検出するため、デフォルトでは Pandora FMS サーバによって配布される、パッケージとアプリケーション名を様々な CVE と関連付けるデータベースを利用します。リモートで脆弱性を検知するため CPE と CVE を関連付けるデータベースが利用されます。コンソールはサーバデータベースで見つかった様々な CVE 情報を含むデータベースを利用し、ユーザへの表示とレポート生成を行います。様々な CVE データはバージョン774から存在する `tpandora_cve` テーブルから読み込まれます。

脆弱性監査の設定

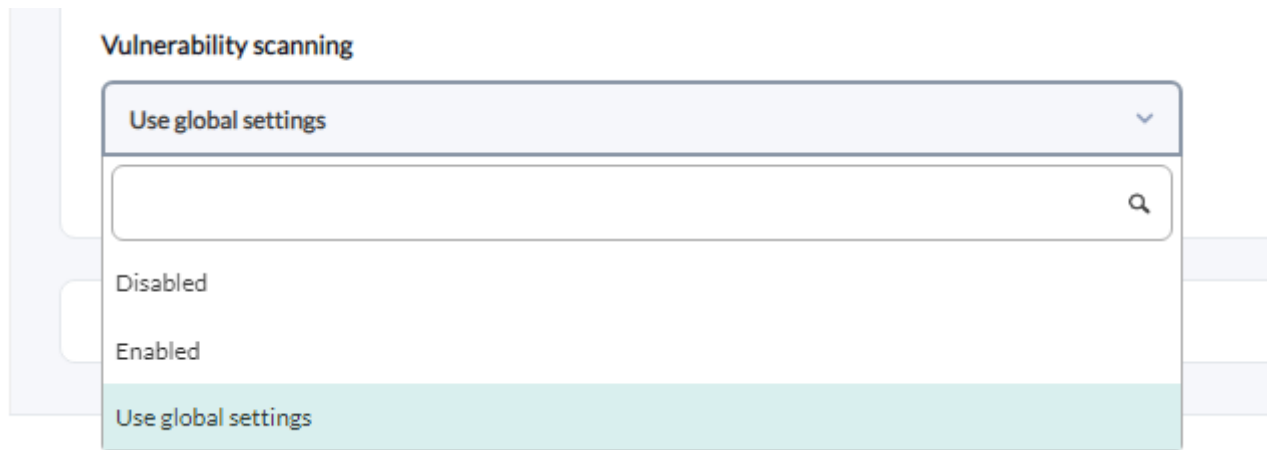
サーバでの設定

ローカルな脆弱性検知のためには、**データサーバ**がアクティブでエンドポイントが**インベントリ情報**を送信している必要があります。

リモート脆弱性検知のためには**自動検出サーバ**が**有効**である必要があります。

エージェントでの設定

エージェントを手動で無効化または有効化することも、**詳細設定セクション**のグローバル設定を(デフォルトで)使用することもできます。



リモートスキャンタスク

これを利用するためには、**自動検出**に進み新たに脆弱性検出タスクを立ち上げる必要があります。脆弱性検出を始めるために、既存の1つ以上のグループを選択するよう求められます。スキャンには各エージェントのメイン IP アドレスが使用されます。監視していない、または Pandora FMS に存在しない対象の場合は、はじめに通常のネットワーク検出で検出しておく必要があります。

脆弱性スキャンは新しいエージェントを作成しません。

Applications

DB2 (legacy)

Microsoft SQL Server (legacy)

MySQL (legacy)

Oracle (legacy)

VMware (legacy)

DB2

Vulnerability Scanner

*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

脆弱性データ表示

情報を取得できると各監視システムに脆弱性のタブが表示されます。

バージョン775現在ダッシュボードが表示され、(脆弱性ランキングで最低の)最も脆弱なシステムトップ10、(最も頻出の)脆弱性トップ10、その他グルーピングのグラフが含まれています。

これらのレポートはいくつかの要素でフィルタできます。

- 機器のグループ
- 攻撃の複雑さ(低/中/高)
- 脆弱性の種類(機密性、完全性、可用性、...)
- アクセスベクトル(ネットワーク、隣接ネットワーク、...)
- ユーザ操作(なし、必要、など)
- 必要な権限(なし、低、...)

The screenshot displays the Pandora FMS dashboard interface. At the top, there is a navigation bar with various icons, including a red-bordered icon representing agent contact. The main content area is divided into several sections:

- Agent contact:** This section provides details for a specific agent. It includes:
 - Interval: 5 minutes
 - Lastcontact / Remote: 3 minutes 43 seconds / November 8, 2023, 11:08 am
 - Next contact: A progress bar showing 221 s remaining.
 - Group: Servers
 - Secondary groups: N/A
 - Parent: N/A
 - Last status change: 8 minutes 46 seconds
- Agent access rate (Last 24h):** A bar chart showing access rates over time. The x-axis has labels for 07:11, 10:11, and 11:11. The y-axis ranges from 0 to 3.0. There are two prominent green bars, one around 10:11 and another around 11:11.

At the bottom of the dashboard, there are control elements:

- Module group:** A dropdown menu currently set to "All".
- Show in hierarchy mode:** A toggle switch.
- Reset:** A button with a circular arrow icon.
- Filter:** A button with a magnifying glass icon.

Summary

System risk

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

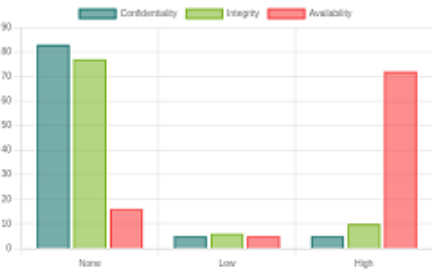
93 vulnerabilities with moderate impact require attention.

4.66 Medium risk

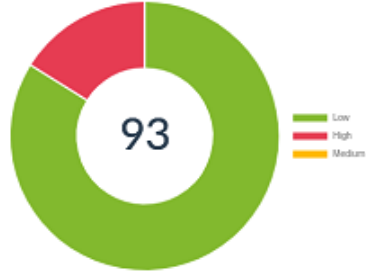
0 Healthy

High risk 10

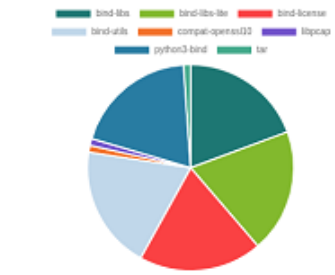
Severity



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

Search input field for 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

スコープメトリクスで脆弱性を素早くフィルタできます。

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 | 👁️ |

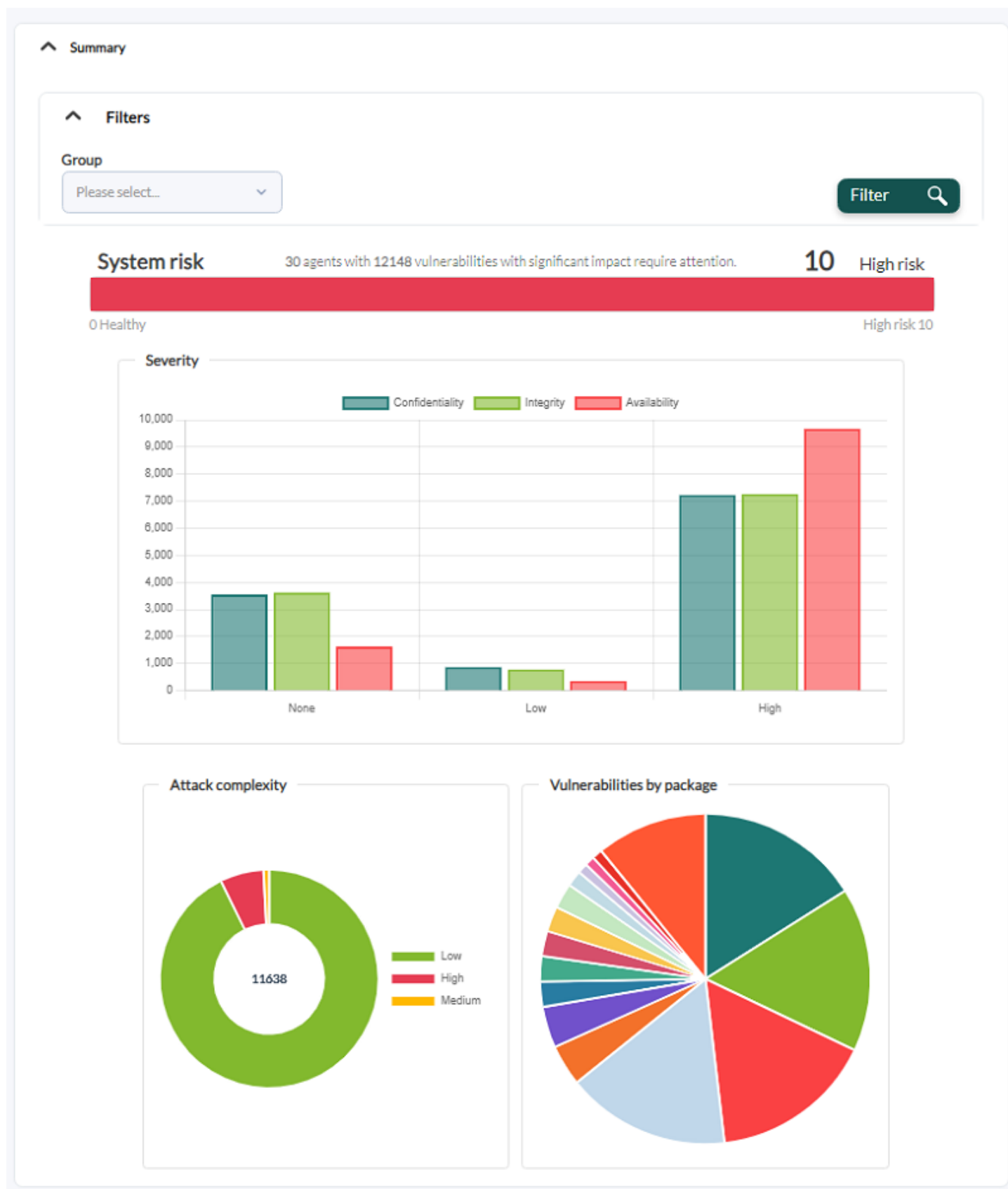
25 CSV

戦略的セキュリティの表示

操作(Operation) セキュリティ(Security) 脆弱性(Vulnerabilities) メニューに進みます。

概要

エージェントの全体像が表示され、システム全体のリスク、攻撃の複雑さの重大度、インストールされている各ソフトウェアパッケージがもたらす脆弱性をまとめたグラフが表示されます。



エージェントグループでフィルタできます。デフォルトでは全て(All)のグループが表示されます。

データの内訳

セキュリティデータの内訳として、最も脆弱であるトップ10のエージェントとトップ10のソフトウェアパッケージを表示します。


^ Data breakdown


^ Filters




Group
Please select... Filter



| ▲ Agent | Vulnerabilities | Risk |
|--------------------------|-----------------|------|
| 83etc | 410 | 10 |
| 257f378d433124706d442bbb | 394 | 10 |
| fa2025fd2f64462a43d94fae | 394 | 10 |
| 4012470edc77bc97f58b3f80 | 410 | 10 |
| bf78e4ac01eb3144b5f3cf5 | 394 | 10 |
| 9daa3ecee84ed039bcf2efdc | 394 | 10 |
| 602ef1ca527c0bb7d144bf0a | 410 | 10 |
| 64ab08385a39067b8161cb68 | 410 | 10 |
| bec95961964493dbca9cf544 | 394 | 10 |
| 0f0d005d0d9f31afcf979437 | 396 | 10 |





| ▲ 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 

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 |  |

情報はエージェントグループでのフィルタと CSV フォーマットでのエクスポートが可能です。必要な権限 ユーザ操作 攻撃ベクトルの項は [監査](#) セクションを参照するボタンがあります。

監査

デフォルトでは全ての脆弱性情報を表示するので、ロードに時間がかかるかもしれません CVE 番号を含む脆弱性の特徴の組み合わせでフィルタすることができます。

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

情報をフィルタすると、各アイテムに詳細な情報を表示するボタン(目のアイコン)が現れます。

[Pandora FMS ドキュメント一覧に戻る](#)