



## Red Hat Insights 2022

### 脆弱性サービスレポートの生成

CVE セキュリティーの脆弱性に晒された RHEL システムの通知



## Red Hat Insights 2022 脆弱性サービスレポートの生成

---

CVE セキュリティーの脆弱性に晒された RHEL システムの通知

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

## 法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Generating\_Vulnerability\_Service\_Reports.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

脆弱性サービスレポートを生成し、CVE セキュリティーの脆弱性にさらされている RHEL システムを通知します。

---

## 目次

多様性を受け入れるオープンソースの強化 .....	3
RED HAT ドキュメントへのフィードバック .....	4
第1章 RHEL VULNERABILITY サービスのレポート用の INSIGHTS の概要 .....	5
第2章 エグゼクティブレポート .....	6
2.1. エグゼクティブレポートのダウンロード .....	6
2.2. VULNERABILITY サービス API を使用したエグゼクティブレポートのダウンロード .....	6
第3章 CVE による報告 .....	8
3.1. CVE の PDF レポートの作成 .....	9
第4章 JSON、CSV、または PDF ファイルとしての VULNERABILITY データのエクスポート .....	11
4.1. VULNERABILITY サービスからの CVE データのエクスポート .....	11
第5章 参考資料 .....	12



## 多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[弊社の CTO、Chris Wright のメッセージ](#) を参照してください。

## RED HAT ドキュメントへのフィードバック

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックを提供するには、ドキュメントのテキストを強調表示し、コメントを追加します。

### 前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルでは、このドキュメントは **Multi-page HTML** 表示形式です。

### 手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。



#### 注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題リンクをクリックします。



## 第1章 RHEL VULNERABILITY サービスのレポート用の INSIGHTS の概要

DevOps チーム、セキュリティーチーム、エグゼクティブチームなどのさまざまなステークホルダーに、インフラストラクチャーのセキュリティー脆弱性を伝達する機能は極めて重要です。Vulnerability サービスを使用すると、以下のレポートをダウンロードしてオフラインの分析や、他のユーザーとの共有を行うことができます。

- **Executive Reports:**エグゼクティブに向けたインフラストラクチャーのセキュリティー脆弱性に関する PDF 形式のサマリーおよび概要
- **CVE reports:**インフラストラクチャーが晒されている CVE を選択したり、フィルタリングした PDF 形式のレポート。脆弱性データのハイライトおよび共有が目的。
- **Vulnerability data export** エクスポートの実行時に設定したフィルターをもとに選択した CVE データの JSON または CSV ファイルへのエクスポート。

## 第2章 エグゼクティブレポート

インフラストラクチャーでのセキュリティ脆弱性をまとめた概要エグゼクティブレポートをダウンロードできます。エグゼクティブレポートは、エグゼクティブを対象として設計された 2-3 ページの PDF ファイルで、以下の情報が含まれます。

### ページ 1

- 分析する RHEL システムの数
- システムが現在影響を受ける個別の CVE 数
- インフラストラクチャー内のセキュリティールールの数

### ページ 2

- 重大度別の CVE の割合 (CVSS ベーススコア範囲)
- 7、30、および 90 日間に公開された CVE の数
- セキュリティールールや既知の不正使用など、インフラストラクチャー内で上位 3 つの CVE

### ページ 3

- 重大度別のセキュリティールールの内訳
- 上位 3 つのセキュリティールール (重大度やセキュリティーリスクに晒されているシステムの数を含む)

## 2.1. エグゼクティブレポートのダウンロード

以下の手順に従い、レポートをダウンロードします。

### 手順

1. 必要に応じて、[Red Hat Enterprise Linux > Vulnerability > Reports](#) タブに移動し、ログインします。
2. **Executive report** カードで、**Download PDF** をクリックします。
3. **Save File**、**OK** の順にクリックします。

### 検証

1. PDF ファイルが **Downloads** フォルダーまたは指定した場所にあることを確認します。

## 2.2. VULNERABILITY サービス API を使用したエグゼクティブレポートのダウンロード

[Vulnerability サービス API](#) を使用してレポートをダウンロードできます。

- 要求 URL: <https://console.redhat.com/api/vulnerability/v1/report/executive>
- Curl:

```
curl -X GET "https://console.redhat.com/api/vulnerability/v1/report/executive" -H "accept: application/vnd.api+json"
```

## 第3章 CVE による報告

システムが影響を受ける CVE のフィルターされた一覧を示す PDF レポートを作成できます。各レポートに、関連する名前を付け、フィルターを適用し、ユーザーノートを追加して、集中データを特定のステークホルダーに表示します。

PDF レポートを設定する際に、以下のフィルターを適用できます。

- **Security rules.**セキュリティールールラベルの付いた CVE のみを表示します。
- **既知の不正使用**既知の不正使用ラベルの付いた CVE のみを表示します。
- **Severity.**1 つ以上の値 (Critical、Important、Moderate、Low、または Unknown) を選択します。
- **CVSS base score.**1 つ以上の範囲を選択します。All、0.0-3.9、4.0-7.9、8.0-10.0、N/A (該当なし)
- **Business risk.**1 つ以上の値を選択します (High、Medium、Low、Not defined)。
- **Status.**1 つ以上の値を選択します。Not reviewed、In review、On-hold、Scheduled for patch、Resolved、No action - risk accepted、Resolved via mitigation
- **Publish date.**All、Last 7 days、Last 30 days、Last 90 days、Last year、または More than 1 year から選択します。
- **OS に適用されます。**フィルターして表示するシステムの RHEL マイナーバージョンを選択します。
- **Tags.**タグ付けされたシステムのグループを選択します。タグおよびシステムグループの詳細は、[Chapter 4, System tags and groups, Assessing and Monitoring Security Vulnerabilities on RHEL Systems](#) を参照してください。

CVE レポートでは、CVE と、Red Hat CVE データベースで該当する CVE ページへのリンクが記載されるため、各 CVE の詳細を確認できます。このリストは、主に CVE の公開日によって順序付けられ、リストの上部に最新の CVE が公開されます。

### Insights 脆弱性 CVE レポートの例



## Insights Vulnerability CVE Report

This is a summary of CVEs identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) systems.

This report includes CVEs with a CVSS base score of 0.0 - 10.0; published anytime.

These CVEs apply to systems in your inventory tagged with `satellite:activation_key=RHEL8_AK`.

The vulnerability service identified 625 CVEs within this criteria that impact at least one of your 17 analyzed RHEL systems. Of the identified CVEs, 4 CVEs have a known exploit.

CVE ID	Publish date	CVSS base score	Severity	Systems exposed	Business risk	Status
<a href="#">CVE-2019-18218</a>	25 Aug 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25038</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25032</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25036</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25042</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25039</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25034</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2019-25035</a>	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
<a href="#">CVE-2020-9850</a> <b>Known exploit</b>	09 July 2020	9.8	Moderate	3	Not defined	Not reviewed
<a href="#">CVE-2020-9895</a>	28 July 2020	9.8	Moderate	3	Not defined	Not reviewed

**Known exploit:** This CVE is identified with a "Known exploit" label because Red Hat has determined this CVE has a public exploit. This CVE is unpatched on your system. CVEs with this label should be addressed with high priority due to the risks posed by them. "Known exploit" does not mean we have taken steps to determine if the CVE has been exploited in your environment.

**Security rule:** Indicates a security rule associated with this CVE. Security rules are written by Red Hat to help you configure your systems.

### 3.1. CVE の PDF レポートの作成

以下の手順に従って、お使いのシステムに影響する可能性がある CVE の特定の時点のスナップショットを作成します。

#### 前提条件

- [Red Hat Hybrid Cloud コンソール](#) にログインしている必要があります。

#### 手順

1. Insights for RHEL アプリケーションの [Red Hat Enterprise Linux > Vulnerability > Reports](#) ページに移動します。
2. **Report by CVEs** カードで、**Create report** をクリックします。
3. 必要に応じてポップアップカードで選択します。

Report by CVEs ×

Report title

Insights Vulnerability CVE Report

Filter CVEs by

Security rule: All ▼

Known exploit: All ▼

Severity: All ▼

CVSS base score: All ▼

Business risk: All ▼

Status: All ▼

Publish date: All ▼

Applies to OS: Any ▼

Applying to systems in your inventory meeting these criteria

Tags: All ▼

CVE data to include

All columns

Choose columns

Sort CVEs by

CVSS base score: High to Low (Default) ▼

User notes (optional)

Export report

Cancel

- a. 必要に応じて、レポートタイトルをカスタマイズします。
  - b. **Filter CVEs by** で、各フィルターのドロップダウンメニューをクリックして値を選択します。
  - c. **Tags** を選択して、タグ付けしたシステムグループのシステムのみ含めます。
  - d. 追加する CVE データでは、デフォルトで **選択列** がアクティブになっており、追加しない列の選択を解除できます。すべてのボックスにチェックマークを入れたままにするか、**All columns** をクリックしてすべてを表示します。
  - e. 必要に応じて、注記を追加して、対象対象オーディエンスのレポートコンテキストを指定します。
4. **Export report** をクリックし、アプリケーションによる、レポートの作成時間を許可します。
  5. OS が要求されたら PDF ファイルを開くか、保存し、**OK** をクリックします。

## 第4章 JSON、CSV、または PDF ファイルとしての VULNERABILITY データのエクスポート

Vulnerability サービスを使用すると、RHEL インフラストラクチャーのシステムで CVE のデータをエクスポートできます。Vulnerability サービスでフィルターを適用して、特定の CVE またはシステムセットを表示すると、このフィルターの基準をもとにデータをエクスポートできます。

これらのレポートには Insights for Red Hat Enterprise Linux アプリケーションからアクセスでき、.csv、.json、または PDF ファイルとしてエクスポートおよびダウンロードできます。

### 4.1. VULNERABILITY サービスからの CVE データのエクスポート

Vulnerability サービスから一部のデータをエクスポートするには、以下の手順を実行します。

#### 手順

1. 必要に応じて [Red Hat Enterprise Linux > Vulnerability > CVEs](#) ページに移動し、ログインします。
2. フィルターを適用し、各列の上部にあるソート機能を使用して、特定の CVE を見つけます。
3. CVE の一覧および Filters メニューの右側にある **Export** アイコン  をクリックし、ダウンロード設定に基づいて **Export to JSON**、**Export to CSV**、または **Export as PDF** を選択します。
4. ダウンロード先を選択し、**Save** をクリックします。

## 第5章 参考資料

Vulnerability サービスや他の Insights for Red Hat Enterprise Linux サービスおよび機能に関する詳細は、以下の資料をご利用いただけます。

- [RHEL システムでのセキュリティー脆弱性の評価および監視](#)
- [Vulnerability Service と Ansible Playbook を使用したセキュリティーエクスポージャーの修正](#)
- [Insights for Red Hat Enterprise Linux ドキュメント](#)
- [Insights for Red Hat Enterprise Linux 製品サポートページ](#)