



Red Hat Insights 1-latest

Vulnerability 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 1-latest Vulnerability 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

法律上の通知

Copyright © 2024 Red Hat, Inc.

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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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。Red Hat では、コード、ドキュメント、Web プロパティー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、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

目次

第1章 INSIGHTS FOR RED HAT ENTERPRISE LINUX 脆弱性サービスレポートの概要	3
第2章 エグゼクティブレポート	4
2.1. エグゼクティブレポートのダウンロード	4
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	4
第3章 CVE による報告	6

第1章 INSIGHTS FOR RED HAT ENTERPRISE LINUX 脆弱性サービスレポートの概要

DevOps チーム、セキュリティチーム、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で分析したり、他のユーザーと共有することができます。

- **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
- アドバイザリーがある CVE のリスト

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ル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. [Security > Vulnerability > Reports](#) タブに移動し、必要に応じてログインします。
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リストを示す 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:** セキュリティーラベルの付いた CVE のみを表示します。
- **Known exploit:** 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 ベーススコア:** All、0.0-3.9、4.0-7.9、8.0-10.0、N/A (該当なし) から、1つまたは複数の範囲を選択します。
- **ビジネスリスク:** High、Medium、Low、Not defined から、1つまたは複数の値を選択します。
- **Status:** Not reviewed、In review、On-hold、Scheduled for patch、Resolved、No action - risk accepted、Resolved via mitigation から、1つまたは複数の値を選択します。
- **Publish date:** 以下から選択します (All、Last 7 days、Last 30 days、Last 90 days、Last year、More than 1 year)。
- **Applies to OS:** 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、[システムタグとグループ](#) を参照してください。