# Red Hat Enterprise Linux 8

## セキュリティー更新の管理および監視

Red Hat Enterprise Linux 8 でセキュリティー更新の管理および監視を行うためのガイド

Last Updated: 2021-08-30

# Red Hat Enterprise Linux 8 セキュリティー更新の管理および監視

Red Hat Enterprise Linux 8 でセキュリティー更新の管理および監視を行うためのガイド

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



## 概要

本書では、セキュリティー更新の概要およびインストール方法、ならびにその更新に関する追加情報を表示する方法を説明します。

# 目次

# 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、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 (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
  1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上端に **Feedback** ボタンがあることを確認してください。
  2. マウスカーソルで、コメントを追加する部分を強調表示します。
  3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
  4. 表示される手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
  1. Bugzilla の Web サイトにアクセスします。
  2. Component で **Documentation** を選択します。
  3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
  4. **Submit Bug** をクリックします。

# 第1章 セキュリティー更新の特定

エンタープライズシステムは、現在および今後の脅威から安全に保つために、通常のセキュリティー更新が必要です。Red Hat Product Security チームは、エンタープライズソリューションを確実にデプロイおよび維持するのに必要なガイダンスを提供します。

## 1.1. セキュリティーアドバイザリーとは

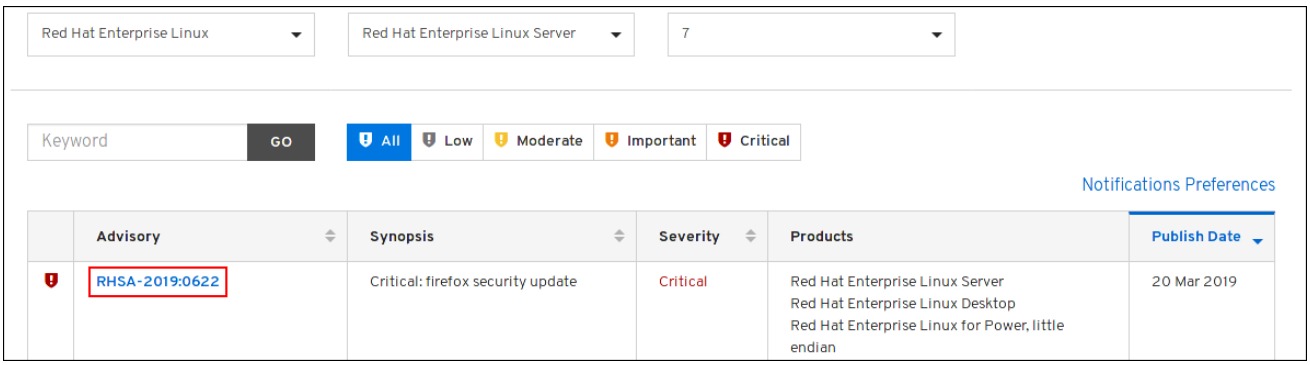
Red Hat Security Advisories (RHSA) では、Red Hat 製品およびサービスで修正されたセキュリティーの不具合に関する情報が記載されています。

各 RHSA には、以下の情報が含まれています。

- 重大度
- タイプおよびステータス
- 影響を受ける製品
- 修正された問題の概要
- その問題に関するチケットへのリンク。すべてのチケットが公開されているわけではないことに注意してください。
- CVE (Common Vulnerabilities and Exposures) 番号および攻撃の複雑性などの追加情報へのリンク。

Red Hat カスタマーポータルでは、Red Hat が公開している Red Hat Security Advisory の一覧を提供しています。Red Hat セキュリティーアドバイザリーの一覧からアドバイザリーの ID に移動して、特定のアドバイザリーの詳細を表示できます。

**図1.1 セキュリティーアドバイザリーの一覧**




必要に応じて、特定の製品、バリアント、バージョン、およびアーキテクチャーで結果を絞り込むこともできます。たとえば、Red Hat Enterprise Linux 8 のアドバイザリーのみを表示するには、以下のフィルターを設定します。

- 製品: Red Hat Enterprise Linux
- バリアント: すべてのバリアント
- バージョン: 8
- または、8.2 などのマイナーバージョンを選択します。

**関連情報**

- List of Red Hat Security Advisories
- Anatomy of a Red Hat Security Advisory
- Red Hat カスタマーポータル

## 1.2. ホストにインストールされていないセキュリティー更新の表示

**yum** ユーティリティーを使用して、お使いのシステムで利用可能なセキュリティー更新の一覧を表示できます。

**前提条件**

- ホストに割り当てられている Red Hat サブスクリプション

**手順**

- ホストにインストールされていない、利用可能なセキュリティー更新の一覧を表示します。

```
# yum updateinfo list updates security
...
RHSA-2019:0997 Important/Sec. platform-python-3.6.8-2.el8_0.x86_64
RHSA-2019:0997 Important/Sec. python3-libs-3.6.8-2.el8_0.x86_64
RHSA-2019:0990 Moderate/Sec.  systemd-239-13.el8_0.3.x86_64
...
```

## 1.3. ホストにインストールされているセキュリティー更新の表示

**yum** ユーティリティーを使用して、お使いのシステムでインストールしたセキュリティー更新を一覧表示できます。

**手順**

- ホストにインストールされているセキュリティー更新の一覧を表示します。

```
# yum updateinfo list security installed
...
RHSA-2019:1234 Important/Sec. libssh2-1.8.0-7.module+el8+2833+c7d6d092
RHSA-2019:4567 Important/Sec. python3-libs-3.6.7.1.el8.x86_64
RHSA-2019:8901 Important/Sec. python3-libs-3.6.8-1.el8.x86_64
...
```

1 つのパッケージに含まれる複数の更新がインストールされている場合は、**yum** で、そのパッケージのアドバイザリーがすべて表示されます。上記の例では、システムインストール以降、**python3-libs** パッケージのセキュリティー更新が 2 つインストールされています。

## 1.4. YUM を使用して特定のアドバイザリーを表示

**yum** ユーティリティーを使用して、更新で利用可能な特定のアドバイザリー情報を表示します。

**前提条件**

- ホストに割り当てられている Red Hat サブスクリプション
- セキュリティーアドバイザリーの **Update ID** がある。「セキュリティーアドバイザリーの更新の特定」を参照してください。
- そのアドバイザリーが提供する更新がインストールされていない。

**手順**

- 特定のアドバイザリーを表示します。

```
# yum updateinfo info <Update ID>
==============================================================================
  Important: python3 security update
==============================================================================
  Update ID: RHSA-2019:0997
       Type: security
    Updated: 2019-05-07 05:41:52
       Bugs: 1688543 - CVE-2019-9636 python: Information Disclosure due to urlsplit improper
NFKC normalization
       CVEs: CVE-2019-9636
Description: ...
```

**Update ID** を必要なアドバイザリーに置き換えます。たとえば、**# yum updateinfo info <RHSA-2019:0997>** になります。

# 第2章 セキュリティー更新のインストール

## 2.1. 利用可能なすべてのセキュリティー更新のインストール

システムのセキュリティーを最新の状態に維持するには、**yum** ユーティリティーを使用して、現在利用可能なすべてのセキュリティー更新をインストールできます。

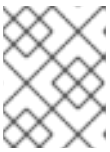
**前提条件**

- ホストに割り当てられている Red Hat サブスクリプション

**手順**

1. **yum** ユーティリティーを使用してセキュリティー更新をインストールします。

```
# yum update --security
```



**注記**

**--security** パラメーターは重要です。これを使用しないと、**yum update** により、バグ修正や機能強化など、すべてのアップデートがインストールされます。

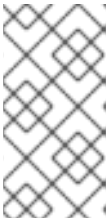
2. **y** を押してインストールを確認し、起動します。

```
...
Transcription Summary
==========================================
Upgrade  ... Packages

Total download size: ... M
Is this ok [y/d/N]: y
```

3. 必要に応じて、更新したパッケージのインストール後に、システムの手動再起動を必要とするプロセスの一覧を表示します。

```
# yum needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```



**注記**

このコマンドは、サービスではなく、再起動が必要なプロセスのみを一覧表示します。つまり、**systemctl** ユーティリティーを使用して一覧表示されるプロセスを再起動することはできません。たとえば、このプロセスを所有するユーザーがログアウトすると、この出力内の **bash** プロセスは終了します。

## 2.2. 特定のアドバイザリーが提供するセキュリティー更新のインストール

特定の状況では、特定の更新のみをインストールする場合があります。たとえば、ダウンタイムをスケジュールせずに特定のサービスを更新できる場合は、このサービスにのみセキュリティー更新をインストールし、後で残りのセキュリティー更新をインストールできます。

**前提条件**

- ホストに割り当てられている Red Hat サブスクリプション
- セキュリティーアドバイザリーの更新 ID がある。「セキュリティーアドバイザリーの更新の特定」を参照してください。

**手順**

1. 特定のアドバイザリーをインストールします。

```
# yum update --advisory=<Update ID>
```

Update ID を必要なアドバイザリーに置き換えます。たとえば、**#yum update --advisory=<RHSA-2019:0997>** となります。

2. **y** を押してインストールを確認し、起動します。

```
...
Transaction Summary
==========================================
Upgrade  ... Packages

Total download size: ... M
Is this ok [y/d/N]: y
```

3. 必要に応じて、更新されたパッケージのインストール後にシステムを手動で再起動する必要のあるプロセスの一覧を表示します。

```
# yum needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```

**注記**

このコマンドは、サービスではなく、再起動が必要なプロセスのみを一覧表示します。これは、**systemctl** ユーティリティーを使用して一覧表示されているプロセスをすべて再起動できないことを意味します。たとえば、このプロセスを所有するユーザーがログアウトすると、この出力内の **bash** プロセスは終了します。

## 2.3. 関連情報

- ワークステーションおよびサーバーのセキュリティー保護に関する詳細は、RHEL 8 の『セキュリティーの強化』を参照してください。
- Security-Enhanced Linux の詳細は、RHEL 8 の『SELinux の使用』を参照してください。