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: 2020-09-04

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

法律上の通知

概要

本書は、セキュリティー更新の概要、インストール方法、および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

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

本章では、**セキュリティーアドバイザリー** の用語について詳しく説明し、利用可能なセキュリティー更新とインストール済みのセキュリティー更新の一覧を表示する方法を説明します。

1.1. セキュリティーアドバイザリーとは

Red Hat は、セキュリティーアドバイザリーの形で、Red Hat の製品およびサービスに影響を及ぼすセキュリティーの欠陥に関する情報を提供します。

RHSA (Red Hat Security Advisories) には、以下のような重要な情報が含まれます。

- 重大度
- 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 番号と、攻撃の複雑性などの詳細が記載されたページへのリンク

関連情報

- Red Hat Security Advisory の一覧

1.2. 利用可能なセキュリティー更新の表示

以下の手順に従って、**yum** ユーティリティーを使用して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します。

前提条件

- 有効な Red Hat サブスクリプションがホストに割り当てられている。

手順

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

```
$ sudo 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

Red Hat Enterprise Linux 8 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する場合は、**yum updateinfo list security installed** コマンドを使用します。

手順

1. 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。

```
$ sudo 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 つのパッケージで、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。上の例では、Red Hat Enterprise Linux 8 のインストール以降、**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。

第2章 セキュリティーアドバイザリーの表示

本章では、RHSA (Red Hat Security Advisories) に関する情報が記載されている場所と、アドバイザリーを表示する方法を説明します。

2.1. カスタマーポータルでセキュリティー更新の表示

Red Hat は、Red Hat カスタマーポータルでセキュリティーアドバイザリーを公開しています。本セクションでは、アドバイザリーの場所と、アドバイザリーにフィルターをかけて表示する方法を説明します。

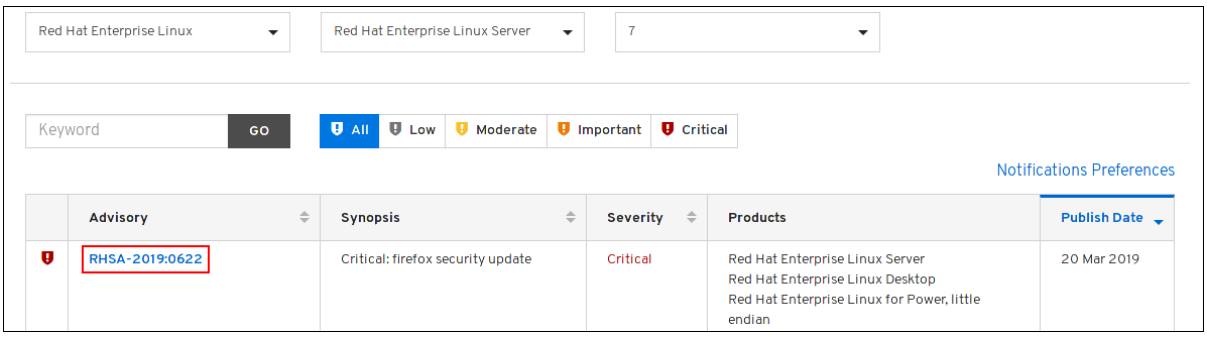
手順

1. ブラウザーで、Security Advisories を開きます。
   このページには、Red Hat が公開しているセキュリティーアドバイザリーがすべて表示されます。

2. 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フィルターをかけます。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。

3. 特定のアドバイザリーの詳細を表示する場合は、表に記載されるアドバイザリーの ID をクリックします。



2.2. YUM を使用して特定のアドバイザリーを表示

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場合は、**yum** ユーティリティーを使用して、そのアドバイザリーを表示します。

前提条件

- 有効な Red Hat サブスクリプションがホストに割り当てられている。
- セキュリティーアドバイザリーの ID が分かっている。ホストにインストールされているセキュリティー更新と、利用可能なセキュリティー更新のアドバイザリーを表示する方法は、*1章 セキュリティー更新の特定*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

1. アドバイザリーを表示します。たとえば、アドバイザリー **RHSA-2019:0997** の詳細を表示するには、以下のコマンドを実行します。

```
$ sudo yum updateinfo info RHSA-2019:0997
==============================================================================
====
  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: ...
```

第3章 セキュリティー更新のインストール

本章では、Red Hat Enterprise Linux 8 にセキュリティー更新をインストールする方法を説明します。

前提条件

- 有効な Red Hat サブスクリプションがホストに割り当てられている。

3.1. 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

本セクションでは、ホストで利用可能なセキュリティー更新をすべてインストールする方法を説明します。

手順

1. セキュリティー更新をすべてインストールするには、以下のコマンドを入力します。

```
$ sudo yum update --security
```

   --security パラメーターを使用しないと、**yum** は、バグ修正および機能強化が含まれる更新もインストールします。

2. **y** を押して、インストールを起動します。

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

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

3. 必要に応じて、更新したパッケージのインストール後に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。

```
$ sudo yum needs-restarting
```

関連情報

- 「セキュリティー更新の適用後に再起動が必要なサービスの表示」

3.2. 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

たとえば、あるサービスを、ダウンタイムをスケジュールせずに更新できる場合に、管理者が、このサービスのセキュリティー更新のみをインストールし、その他のセキュリティー更新は後でインストールするとします。

本セクションは、特定のセキュリティーアドバイザリーが提供する更新パッケージをインストールする方法を説明します。

前提条件

- 有効な Red Hat サブスクリプションがホストに割り当てられている。

- セキュリティーアドバイザリーの ID が分かっている。ホストにインストールされているセキュリティー更新と、利用可能なセキュリティー更新のアドバイザリーを表示する方法は、1章 *セキュリティー更新の特定*を参照してください。

手順

1. 特定のセキュリティーアドバイザリーが提供するセキュリティー更新をインストールします。たとえば、アドバイザリー **RHSA-2019:0997** が提供する更新をインストールするには、以下のコマンドを実行します。

```
$ sudo yum update --advisory=RHSA-2019:0997
```

2. **y** を押して、インストールを起動します。

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

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

3. 必要に応じて、更新したパッケージのインストール後に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。

```
$ sudo yum needs-restarting
```

関連情報

- 「セキュリティー更新の適用後に再起動が必要なサービスの表示」

第4章 セキュリティー更新の適用後のタスク

Red Hat Enterprise Linux 8 へセキュリティー更新をインストールした後、追加のタスクが必要になる場合があります。本セクションでは、3 つのタスクを説明します。

4.1. セキュリティー更新の適用後に再起動が必要なサービスの表示

Red Hat Enterprise Linux 8 でパッケージを更新する場合は、更新されたライブラリーおよび実行ファイルを使用する特定のプロセスを手動で再起動する必要があります。本セクションでは、このようなプロセスを指定する方法を説明します。

前提条件

- Red Hat Enterprise Linux 8 の更新がインストールされている。詳細は*3章 セキュリティー更新のインストール*を参照してください。

手順

1. 更新前のライブラリーまたは実行ファイルを引き続き使用しているプロセスを一覧表示するには、以下のコマンドを実行します。

```
$ sudo yum needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
...
```

yum needs-restarting コマンドは、サービスではなく、プロセスだけを表示します。これは、**systemctl** ユーティリティーで表示されたプロセスをすべて再起動できるわけでは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** プロセスが終了します。