Red Hat Enterprise Linux 8

セキュリティー更新の管理および監視

RHEL 8 システムのセキュリティーを更新して、攻撃者による既知の問題の悪用を回避する

Last Updated: 2024-06-26

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

RHEL 8 システムのセキュリティーを更新して、攻撃者による既知の問題の悪用を回避する

法律上の通知

概要

セキュリティー更新をインストールし、更新に関する追加の詳細を表示して、新たに発見された脅威や脆弱性から Red Hat Enterprise Linux システムを保護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)

Red Hat 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。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **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追加してください。
5. ダイアログの下部にある **Create** 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を現在および今後の脅威から保護するには、定期的な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

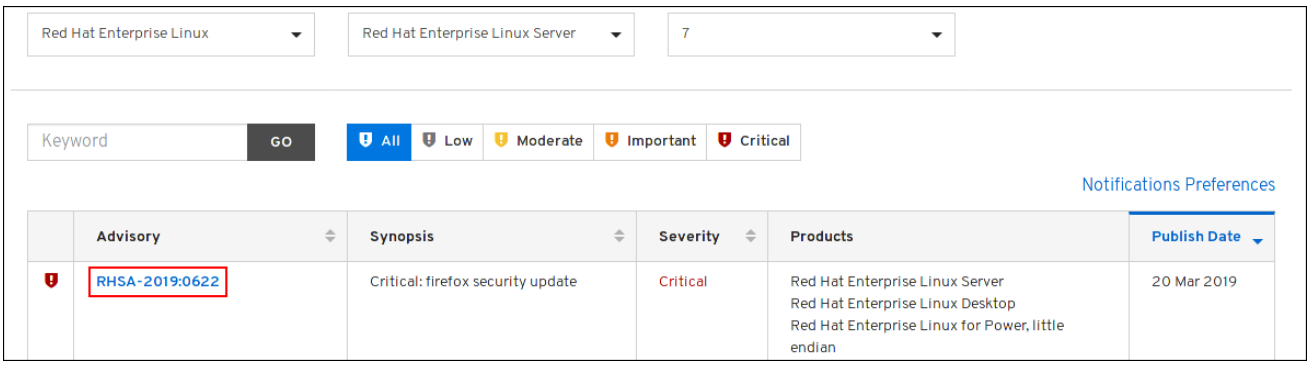
Red Hat セキュリティーアドバイザリー (RHSA) には、Red Hat 製品およびサービスで修正されたセキュリティーの不具合に関する情報が記載されています。

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 セキュリティーアドバイザリー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リスト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リスト



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
- 必要に応じて、8.2 などのマイナーバージョンを選択します。

関連情報

- Red Hat セキュリティーアドバイザリーの一覧
- Red Hat セキュリティーアドバイザリーの構造
- 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リストを表示できます。

前提条件

- 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

- 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リストを表示します。

```
# 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リスト表示できます。

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リストを表示します。

```
# 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. DNF を使用した特定のアドバイザリーの表示

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

- 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 **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

- 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. **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、すべての更新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リストを表示します。

```
# 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リスト表示します。つまり、**systemctl** ユーティリティーを使用してリスト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

状況によっては、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

- 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。
- 更新するセキュリティーアドバイザリーの ID がわかっている。詳細は、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、更新するセキュリティーアドバイザリーの ID に置き換えます。以下に例を示します。

```
# yum update --advisory=RHSA-2019:0997
```

重要

dnf upgrade-minimal --advisory=<Update_ID> コマンドを使用すると、最小限のバージョン変更で特定のアドバイザリーを適用するように更新できます。

2. **y** を押し、インストールを確認して開始します。

```
...
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リストを表示します。

```
# 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リスト表示します。これは、**systemctl** ユーティリティーを使用してリスト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. セキュリティー更新プログラムの自動インストール

すべてのセキュリティー更新を自動的にダウンロードおよびインストールするようにシステムを設定できます。

前提条件

- 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。
- **dnf-automatic** パッケージがインストールされている。

手順

1. **/etc/dnf/automatic.conf** ファイルの **[commands]** セクションで、**upgrade_type** オプションが **default** または **security** に設定されていることを確認します。

```
[commands]
#  What kind of upgrade to perform:
# default                            = all available upgrades
# security                           = only the security upgrades
upgrade_type = security
```

2. **systemd** タイマーユニットを有効にして起動します。

```
# systemctl enable --now dnf-automatic-install.timer
```

検証

1. タイマーが有効化されていることを確認します。

```
# systemctl status dnf-automatic-install.timer
```

関連情報

- **dnf-automatic (8)** man ページ

2.4. 関連情報

- セキュリティーの強化 ドキュメントのワークステーションおよびサーバーのセキュリティーを保護する方法を参照してください。
- Security-Enhanced Linux ドキュメント。