Red Hat Enterprise Linux 9

Gestion et suivi des mises à jour de sécurité

Mise à jour de la sécurité du système RHEL 9 pour empêcher les attaquants d'exploiter les failles connues

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Gestion et suivi des mises à jour de sécurité

Mise à jour de la sécurité du système RHEL 9 pour empêcher les attaquants d'exploiter les failles connues

Notice légale

Résumé

Apprenez à installer les mises à jour de sécurité et à afficher des détails supplémentaires sur les mises à jour afin de protéger vos systèmes Red Hat Enterprise Linux contre les menaces et les vulnérabilités récemment découvertes.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. IDENTIFIER LES MISES À JOUR DE SÉCURITÉ

Le maintien de la sécurité des systèmes d'entreprise contre les menaces actuelles et futures nécessite des mises à jour de sécurité régulières. Red Hat Product Security fournit les conseils dont vous avez besoin pour déployer et maintenir les solutions d'entreprise en toute confiance.

1.1. QU'EST-CE QU'UN AVIS DE SÉCURITÉ ?

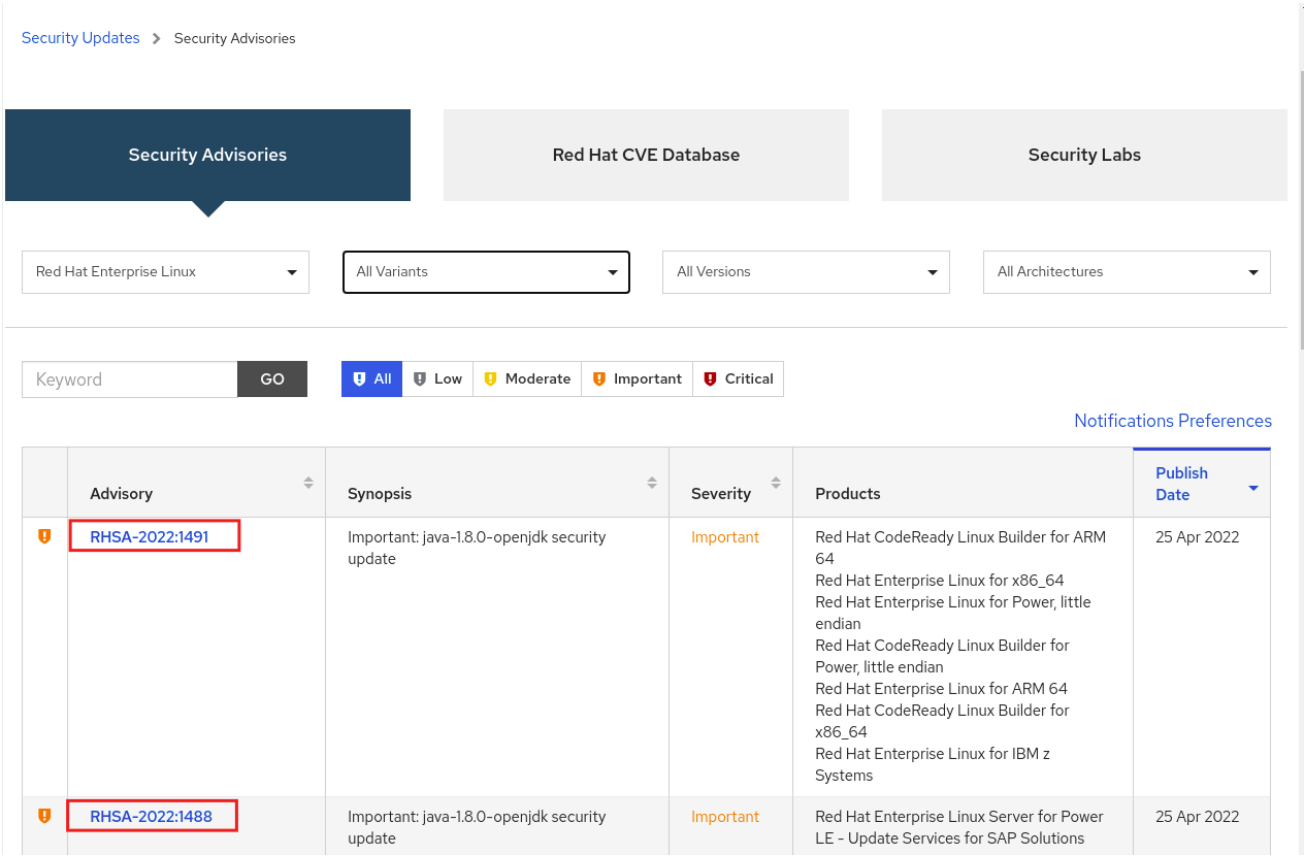
Les avis de sécurité de Red Hat (RHSA) documentent les informations sur les failles de sécurité corrigées dans les produits et services de Red Hat.

Chaque RHSA comprend les informations suivantes :

- Sévérité
- Type et statut
- Produits concernés
- Résumé des problèmes corrigés
- Liens vers les tickets concernant le problème. Notez que tous les tickets ne sont pas publics.
- Numéros de Common Vulnerabilities and Exposures (CVE) et liens avec des détails supplémentaires, tels que la complexité de l'attaque.

Le portail client de Red Hat fournit une liste des avis de sécurité de Red Hat publiés par Red Hat. Vous pouvez afficher les détails d'un avis spécifique en naviguant vers l'ID de l'avis à partir de la liste des avis de sécurité de Red Hat.

Figure 1.1. Liste des avis de sécurité



En option, vous pouvez également filtrer les résultats par produit, variante, version et architecture spécifiques. Par exemple, pour afficher uniquement les avis pour Red Hat Enterprise Linux 9, vous pouvez définir les filtres suivants :

- Produit : Red Hat Enterprise Linux
- Variante : Toutes les variantes
- Version : 9
- Si vous le souhaitez, vous pouvez sélectionner une version mineure.

Ressources supplémentaires

- Liste des avis de sécurité de Red Hat
- Anatomie d'un avis de sécurité de Red Hat
- Portail clients de Red Hat

1.2. AFFICHAGE DES MISES À JOUR DE SÉCURITÉ QUI NE SONT PAS INSTALLÉES SUR UN HÔTE

Vous pouvez dresser la liste de toutes les mises à jour de sécurité disponibles pour votre système à l'aide de l'utilitaire **dnf**.

Prérequis

- Un abonnement Red Hat attaché à l'hôte.

Procédure

- Liste de toutes les mises à jour de sécurité disponibles qui n'ont pas été installées sur l'hôte :

```
# dnf 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. AFFICHAGE DES MISES À JOUR DE SÉCURITÉ INSTALLÉES SUR UN HÔTE

Vous pouvez dresser la liste des mises à jour de sécurité installées sur votre système à l'aide de l'utilitaire **dnf**.

Procédure

- Liste de toutes les mises à jour de sécurité installées sur l'hôte :

```
# dnf 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
...
```

Si plusieurs mises à jour d'un même paquet sont installées, **dnf** répertorie tous les avis relatifs à ce paquet. Dans l'exemple précédent, deux mises à jour de sécurité pour le paquetage **python3-libs** ont été installées depuis l'installation du système.

1.4. AFFICHER UN AVIS SPÉCIFIQUE EN UTILISANT DNF

Vous pouvez utiliser l'utilitaire **dnf** pour afficher une information consultative spécifique disponible pour une mise à jour.

Conditions préalables

- Un abonnement Red Hat attaché à l'hôte.
- Vous avez un avis de sécurité **Update ID**. Voir l'identification des mises à jour de l'avis de sécurité.
- La mise à jour fournie par l'avis n'est pas installée.

Procédure

- Afficher un avis spécifique :

```
# dnf 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: ...
```

Remplacez le site *Update ID* par l'avis requis. Par exemple, **# dnf updateinfo info *<RHSA-2019:0997>***.

CHAPITRE 2. INSTALLATION DES MISES À JOUR DE SÉCURITÉ

2.1. INSTALLATION DE TOUTES LES MISES À JOUR DE SÉCURITÉ DISPONIBLES

Pour maintenir la sécurité de votre système à jour, vous pouvez installer toutes les mises à jour de sécurité disponibles à l'aide de l'utilitaire **dnf**.

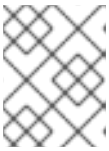
Prérequis

- Un abonnement Red Hat attaché à l'hôte.

Procédure

1. Installez les mises à jour de sécurité à l'aide de l'utilitaire **dnf**:

```
# dnf update --security
```



NOTE

Le paramètre **--security** est important. Sans lui, **dnf update** installe toutes les mises à jour, y compris les corrections de bogues et les améliorations.

2. Confirmez et démarrez l'installation en appuyant sur **y**:

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

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

3. Facultatif : liste des processus qui nécessitent un redémarrage manuel du système après l'installation des paquets mis à jour :

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

NOTE

Cette commande ne répertorie que les processus nécessitant un redémarrage, et non les services. En d'autres termes, vous ne pouvez pas redémarrer les processus répertoriés à l'aide de l'utilitaire **systemctl**. Par exemple, le processus **bash** figurant dans la liste se termine lorsque l'utilisateur propriétaire de ce processus se déconnecte.

2.2. INSTALLATION D'UNE MISE À JOUR DE SÉCURITÉ FOURNIE PAR UN AVIS SPÉCIFIQUE

Dans certaines situations, vous pouvez souhaiter n'installer que des mises à jour spécifiques. Par exemple, si un service spécifique peut être mis à jour sans qu'une interruption de service ne soit programmée, vous pouvez installer les mises à jour de sécurité pour ce seul service, et installer les autres mises à jour de sécurité ultérieurement.

Conditions préalables

- Un abonnement Red Hat attaché à l'hôte.
- Vous disposez d'un avis de sécurité (Security Advisory Update ID). Voir l'identification des mises à jour de l'avis de sécurité.

Procédure

1. Installer un avis spécifique :

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

   Remplacez le site *Update ID* par l'avis requis. Par exemple, **#dnf update --advisory=*<RHSA-2019:0997>***

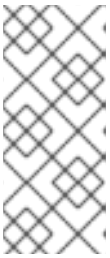
2. Confirmez et démarrez l'installation en appuyant sur **y**:

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

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

3. Facultatif : Dressez la liste des processus qui nécessitent un redémarrage manuel du système après l'installation des paquets mis à jour :

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



NOTE

Cette commande ne répertorie que les processus nécessitant un redémarrage, et non les services. Cela signifie que vous ne pouvez pas redémarrer tous les processus répertoriés à l'aide de l'utilitaire **systemctl**. Par exemple, le processus **bash** figurant dans le résultat est terminé lorsque l'utilisateur propriétaire de ce processus se déconnecte.

2.3. INSTALLATION AUTOMATIQUE DES MISES À JOUR DE SÉCURITÉ

Utilisez la procédure suivante pour mettre à jour automatiquement votre système avec les mises à jour de sécurité.

Conditions préalables

- Un abonnement Red Hat attaché à l'hôte.

Procédure

1. Installer dnf-automatic à l'aide de dnf

```
# dnf install dnf-automatic
```

2. Confirmez et démarrez l'installation en appuyant sur y :

```
...
Transaction Summary
==========================================
Upgrade  ... Packages
Total download size: ... M
Is this ok [y/d/N]: y
```

3. Ouvrez le fichier **/etc/dnf/automatic.conf** dans un éditeur de texte de votre choix, par exemple :

```
# vi /etc/dnf/automatic.conf
```

4. Configurez l'option **upgrade_type = security** dans la section **[commands]**:

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

5. Activer le **systemd timer unit**

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

Ressources supplémentaires

- **dnf-automatic(8)** page de manuel

2.4. RESSOURCES SUPPLÉMENTAIRES

- Voir les pratiques de sécurisation des postes de travail et des serveurs dans le document sur le renforcement de la sécurité.
- Documentation sur le système Linux amélioré sur le plan de la sécurité .