Red Hat Enterprise Linux 8

Gestión y seguimiento de las actualizaciones de seguridad

Guía para la gestión y supervisión de las actualizaciones de seguridad en Red Hat Enterprise Linux 8

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Gestión y seguimiento de las actualizaciones de seguridad

Guía para la gestión y supervisión de las actualizaciones de seguridad en Red Hat Enterprise Linux 8

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.

Legal Notice

Resumen

Este documento describe cómo conocer e instalar las actualizaciones de seguridad, además de mostrar detalles adicionales sobre las mismas.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO

Red Hat se compromete a sustituir el lenguaje problemático en nuestro código, documentación y propiedades web. Estamos empezando con estos cuatro términos: maestro, esclavo, lista negra y lista blanca. Debido a la enormidad de este esfuerzo, estos cambios se implementarán gradualmente a lo largo de varias versiones próximas. Para más detalles, consulte el mensaje de nuestro CTO Chris Wright .

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para comentarios sencillos sobre pasajes concretos:
  1. Asegúrese de que está viendo la documentación en el formato *Multi-page HTML*. Además, asegúrese de ver el botón **Feedback** en la esquina superior derecha del documento.
  2. Utilice el cursor del ratón para resaltar la parte del texto que desea comentar.
  3. Haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado.
  4. Siga las instrucciones mostradas.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
  1. Vaya al sitio web de Bugzilla.
  2. Como componente, utilice **Documentation**.
  3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
  4. Haga clic en **Submit Bug**.

CAPÍTULO 1. IDENTIFICACIÓN DE LAS ACTUALIZACIONES DE SEGURIDAD

En este capítulo se explica el término *security advisories* y se describe cómo se puede mostrar una lista de actualizaciones de seguridad disponibles y ya instaladas.

1.1. ¿QUÉ SON LOS AVISOS DE SEGURIDAD?

Red Hat proporciona información sobre los fallos de seguridad que afectan a los productos y servicios de Red Hat en forma de avisos de seguridad.

Los avisos de seguridad de Red Hat (RHSA) contienen información importante, como:

- Gravedad
- Resumen de los problemas solucionados
- Enlaces a los tickets sobre el problema. Tenga en cuenta que no todos los tickets son públicos.
- Números CVE y enlaces con detalles adicionales, como la complejidad del ataque.

Recursos adicionales

- Lista de avisos de seguridad de Red Hat

1.2. VISUALIZACIÓN DE LAS ACTUALIZACIONES DE SEGURIDAD DISPONIBLES

Utilice este procedimiento para listar las actualizaciones de seguridad disponibles en su sistema con la utilidad **yum**.

Requisitos previos

- Se asigna una suscripción válida de Red Hat al host.

Procedimiento

1. Enumera las actualizaciones de seguridad disponibles para el host que no han sido instaladas:

```
$ 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. VISUALIZACIÓN DE LAS ACTUALIZACIONES DE SEGURIDAD INSTALADAS EN UN HOST

Para mostrar la lista de actualizaciones de seguridad que se han instalado en un host de Red Hat Enterprise Linux 8, utilice el comando **yum updateinfo list security installed**.

Procedimiento

1. Muestra la lista de actualizaciones de seguridad que se han instalado en el host:

```
$ 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
...
```

Si se han instalado varias actualizaciones de un mismo paquete, **yum** lista todos los avisos para el paquete. En el ejemplo anterior, se han instalado dos actualizaciones de seguridad para el paquete **python3-libs** desde la instalación de Red Hat Enterprise Linux 8.

CAPÍTULO 2. VER AVISOS DE SEGURIDAD

Este capítulo describe dónde puede encontrar información sobre los avisos de seguridad de Red Hat (RHSA) y cómo mostrar los avisos.

2.1. VISUALIZACIÓN DE AVISOS EN EL PORTAL DEL CLIENTE

Red Hat publica avisos de seguridad en el Portal del Cliente de Red Hat. Esta sección describe dónde encontrar los avisos y cómo filtrarlos y mostrarlos.

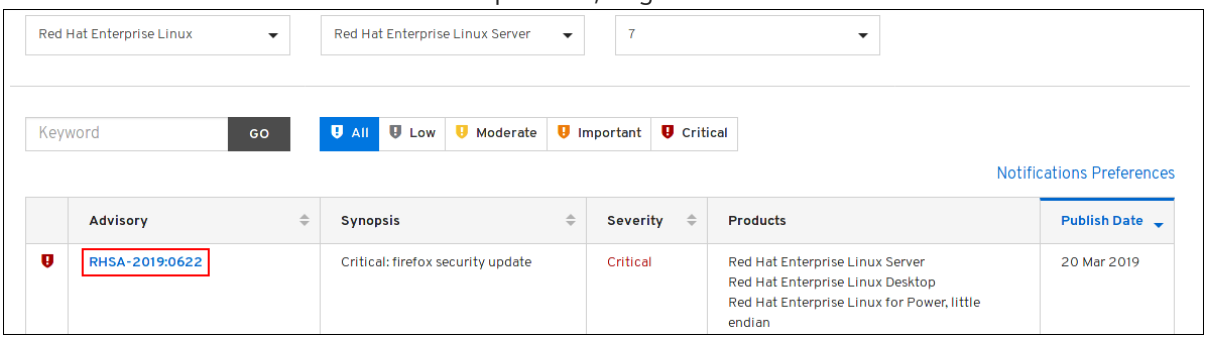
Procedimiento

1. Abra https://access.redhat.com/security/security-updates/ en un navegador.
   Esta página enumera todos los avisos de seguridad publicados por Red Hat.

2. Opcionalmente, filtre por un producto, variante, versión y arquitectura específicos. Por ejemplo, para mostrar sólo los avisos de Red Hat Enterprise Linux 8, establezca los siguientes filtros:

   - Producto: Red Hat Enterprise Linux
   - Variante: Todas las variantes
   - Versión: 8
     Alternativamente, seleccione una versión menor, como la 8.2.

3. Para mostrar los detalles de un aviso específico, haga clic en el ID del aviso en la tabla.



2.2. VISUALIZACIÓN DE UN AVISO ESPECÍFICO MEDIANTE YUM

Si la actualización proporcionada por un aviso no está ya instalada, utilice la utilidad **yum** para mostrar el aviso.

Requisitos previos

- Se asigna una suscripción válida de Red Hat al host.
- Se conoce el ID del aviso de seguridad. Para más detalles sobre la visualización de avisos de actualizaciones de seguridad instaladas y disponibles para el host, consulte Capítulo 1, *Identificación de las actualizaciones de seguridad*.
- La actualización proporcionada por el aviso no está instalada.

Procedimiento

1. Muestra el aviso. Por ejemplo, para mostrar los detalles del aviso **RHSA-2019:0997**:

```
$ 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: ...
```

CAPÍTULO 3. INSTALACIÓN DE ACTUALIZACIONES DE SEGURIDAD

Este capítulo describe cómo instalar actualizaciones de seguridad en Red Hat Enterprise Linux 8.

Requisitos previos

- Se asigna una suscripción válida de Red Hat al host.

3.1. INSTALACIÓN DE TODAS LAS ACTUALIZACIONES DE SEGURIDAD DISPONIBLES

Esta sección describe cómo instalar todas las actualizaciones de seguridad disponibles para un host.

Procedimiento

1. Para instalar todas las actualizaciones de seguridad, entre:

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

   Tenga en cuenta que sin el parámetro **--security**, **yum** instala también actualizaciones que incluyen correcciones de errores y mejoras.

2. Pulse **y** para confirmar e iniciar la instalación:

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

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

3. Opcionalmente, liste los procesos que requieren ser reiniciados manualmente después de instalar los paquetes actualizados:

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

Recursos adicionales

- Sección 4.1, “Visualización de los servicios que requieren un reinicio después de aplicar las actualizaciones de seguridad”

3.2. INSTALACIÓN DE UNA ACTUALIZACIÓN DE SEGURIDAD PROPORCIONADA POR UN AVISO ESPECÍFICO

En ciertas situaciones, por ejemplo, si un servicio específico puede ser actualizado sin programar un tiempo de inactividad, los administradores quieren instalar sólo las actualizaciones de seguridad para este servicio, e instalar todas las demás actualizaciones de seguridad más tarde.

Esta sección explica cómo instalar los paquetes actualizados proporcionados por un aviso de seguridad específico.

Requisitos previos

- Se asigna una suscripción válida de Red Hat al host.
- Se conoce el ID del aviso de seguridad. Para más detalles sobre la visualización de avisos de actualizaciones de seguridad instaladas y disponibles para el host, consulte Capítulo 1, *Identificación de las actualizaciones de seguridad*.

Procedimiento

1. Instale las actualizaciones de seguridad proporcionadas por un aviso de seguridad específico. Por ejemplo, para instalar las actualizaciones proporcionadas por el aviso **RHSA-2019:0997**, introduzca:

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

2. Pulse **y** para confirmar e iniciar la instalación:

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

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

3. Opcionalmente, liste los procesos que requieren ser reiniciados manualmente después de instalar los paquetes actualizados:

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

Recursos adicionales

- Sección 4.1, “Visualización de los servicios que requieren un reinicio después de aplicar las actualizaciones de seguridad”

CAPÍTULO 4. TAREAS ADICIONALES DESPUÉS DE APLICAR LAS ACTUALIZACIONES DE SEGURIDAD

Después de haber instalado las actualizaciones de seguridad en Red Hat Enterprise Linux 8, es posible que necesite realizar tareas adicionales. Esta sección describe estas tareas.

4.1. VISUALIZACIÓN DE LOS SERVICIOS QUE REQUIEREN UN REINICIO DESPUÉS DE APLICAR LAS ACTUALIZACIONES DE SEGURIDAD

Cuando se actualiza un paquete en Red Hat Enterprise Linux 8, ciertos procesos que utilizan bibliotecas y ejecutables actualizados pueden necesitar ser reiniciados manualmente. Esta sección explica cómo identificar estos procesos.

Requisitos previos

- Se han instalado las actualizaciones de Red Hat Enterprise Linux 8. Para más detalles, consulte Capítulo 3, *Instalación de actualizaciones de seguridad*.

Procedimiento

1. Para listar todos los procesos que aún utilizan bibliotecas o ejecutables desde el momento anterior a la actualización:

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

   El comando **yum needs-restarting** sólo muestra los procesos, no los servicios. Esto significa que no puedes reiniciar todos los procesos listados usando la utilidad **systemctl**. Por ejemplo, el proceso **bash** en la salida será terminado cuando el usuario que posee este proceso cierre la sesión.