Red Hat Enterprise Linux 8

Gerenciamento e monitoramento de atualizações de segurança

Um guia para gerenciar e monitorar atualizações de segurança no Red Hat Enterprise Linux 8

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Gerenciamento e monitoramento de atualizações de segurança

Um guia para gerenciar e monitorar atualizações de segurança no 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.

Nota Legal

Resumo

Este documento descreve como aprender e instalar atualizações de segurança, assim como exibir detalhes adicionais sobre as atualizações.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO 3

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT 4

CAPÍTULO 1. IDENTIFICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA 5
1.1. O QUE SÃO CONSELHOS DE SEGURANÇA? 5
1.2. EXIBIÇÃO DAS ATUALIZAÇÕES DE SEGURANÇA DISPONÍVEIS 5
1.3. EXIBINDO ATUALIZAÇÕES DE SEGURANÇA QUE SÃO INSTALADAS EM UM HOST 5

CAPÍTULO 2. CONSULTAS DE SEGURANÇA 7
2.1. EXIBIÇÃO DE AVISOS NO PORTAL DO CLIENTE 7
2.2. EXIBIÇÃO DE UMA ASSESSORIA ESPECÍFICA USANDO O YUM 7

CAPÍTULO 3. INSTALANDO ATUALIZAÇÕES DE SEGURANÇA 9
3.1. INSTALANDO TODAS AS ATUALIZAÇÕES DE SEGURANÇA DISPONÍVEIS 9
3.2. INSTALAÇÃO DE UMA ATUALIZAÇÃO DE SEGURANÇA FORNECIDA POR UMA CONSULTORIA ESPECÍFICA 9

CAPÍTULO 4. TAREFAS ADICIONAIS APÓS A APLICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA 11
4.1. MOSTRAR QUAIS SERVIÇOS PRECISAM SER REINICIADOS APÓS A APLICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA 11

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO

A Red Hat tem o compromisso de substituir a linguagem problemática em nosso código, documentação e propriedades da web. Estamos começando com estes quatro termos: master, slave, blacklist e whitelist. Por causa da enormidade deste esforço, estas mudanças serão implementadas gradualmente ao longo de vários lançamentos futuros. Para mais detalhes, veja a mensagem de nosso CTO Chris Wright.

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT

Agradecemos sua contribuição em nossa documentação. Por favor, diga-nos como podemos melhorá-la. Para fazer isso:

- Para comentários simples sobre passagens específicas:
  1. Certifique-se de que você está visualizando a documentação no formato *Multi-page HTML*. Além disso, certifique-se de ver o botão **Feedback** no canto superior direito do documento.
  2. Use o cursor do mouse para destacar a parte do texto que você deseja comentar.
  3. Clique no pop-up **Add Feedback** que aparece abaixo do texto destacado.
  4. Siga as instruções apresentadas.
- Para enviar comentários mais complexos, crie um bilhete Bugzilla:
  1. Ir para o site da Bugzilla.
  2. Como Componente, use **Documentation**.
  3. Preencha o campo **Description** com sua sugestão de melhoria. Inclua um link para a(s) parte(s) relevante(s) da documentação.
  4. Clique em **Submit Bug**.

CAPÍTULO 1. IDENTIFICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA

Este capítulo desenvolve o termo *security advisories* e descreve como você pode exibir uma lista de atualizações de segurança disponíveis e já instaladas.

1.1. O QUE SÃO CONSELHOS DE SEGURANÇA?

A Red Hat fornece informações sobre falhas de segurança que afetam os produtos e serviços da Red Hat na forma de avisos de segurança.

Os Avisos de Segurança da Red Hat (RHSA) contêm informações importantes, como por exemplo:

- Severidade
- Resumo das questões fixas
- Links para as passagens sobre o problema. Note que nem todos os bilhetes são públicos.
- Números de CVE e links com detalhes adicionais, tais como a complexidade do ataque.

Recursos adicionais

- Lista de Avisos de Segurança da Red Hat

1.2. EXIBIÇÃO DAS ATUALIZAÇÕES DE SEGURANÇA DISPONÍVEIS

Use este procedimento para listar as atualizações de segurança disponíveis em seu sistema com o utilitário **yum**.

Pré-requisitos

- Uma assinatura válida da Red Hat é atribuída ao anfitrião.

Procedimento

1. Liste as atualizações de segurança disponíveis para o host que não foram 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. EXIBINDO ATUALIZAÇÕES DE SEGURANÇA QUE SÃO INSTALADAS EM UM HOST

Para exibir a lista de atualizações de segurança que foram instaladas em um host Red Hat Enterprise Linux 8, use o comando **yum updateinfo list security installed**.

Procedimento

1. Exibir a lista de atualizações de segurança que foram instaladas no 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
...
```

Se várias atualizações de um único pacote tiverem sido instaladas, **yum** lista todos os conselhos para o pacote. No exemplo anterior, duas atualizações de segurança para o pacote **python3-libs** foram instaladas desde a instalação do Red Hat Enterprise Linux 8.

CAPÍTULO 2. CONSULTAS DE SEGURANÇA

Este capítulo descreve onde você pode encontrar informações sobre os Avisos de Segurança da Red Hat (RHSA) e como exibir os avisos.

2.1. EXIBIÇÃO DE AVISOS NO PORTAL DO CLIENTE

A Red Hat publica alertas de segurança no Portal do Cliente da Red Hat. Esta seção descreve onde você encontra os alertas, e como filtrá-los e exibi-los.

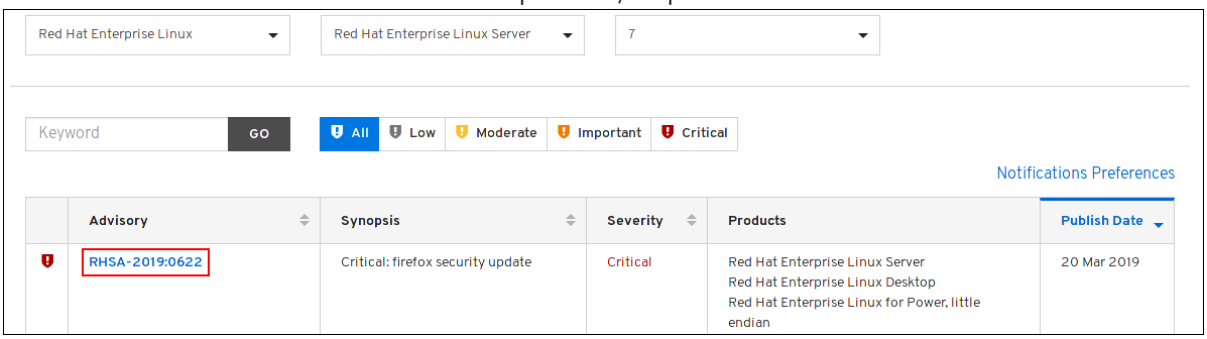
Procedimento

1. Abra https://access.redhat.com/security/security-updates/ em um navegador.
   Esta página lista todos os avisos de segurança Red Hat publicados.

2. Opcionalmente, filtro para um produto específico, variante, versão e arquitetura. Por exemplo, para exibir somente as recomendações para o Red Hat Enterprise Linux 8, defina os seguintes filtros:

   - Produto: Red Hat Enterprise Linux
   - Variante: Todas as Variantes
   - Versão: 8
     Alternativamente, selecione uma versão menor, como a 8.2.

3. Para exibir detalhes de uma assessoria específica, clique no ID da assessoria na tabela.



2.2. EXIBIÇÃO DE UMA ASSESSORIA ESPECÍFICA USANDO O YUM

Se uma atualização fornecida por uma assessoria ainda não estiver instalada, use o utilitário **yum** para exibir a assessoria.

Pré-requisitos

- Uma assinatura válida da Red Hat é atribuída ao anfitrião.
- A identificação da assessoria de segurança é conhecida. Para obter detalhes sobre a exibição das atualizações de segurança instaladas e disponíveis para o host, consulte Capítulo 1, *Identificação de atualizações de segurança*.
- A atualização fornecida pela assessoria não está instalada.

Procedimento

1. Exibir a assessoria. Por exemplo, para exibir os detalhes da assessoria **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. INSTALANDO ATUALIZAÇÕES DE SEGURANÇA

Este capítulo descreve como instalar atualizações de segurança no Red Hat Enterprise Linux 8.

Pré-requisitos

- Uma assinatura válida da Red Hat é atribuída ao anfitrião.

3.1. INSTALANDO TODAS AS ATUALIZAÇÕES DE SEGURANÇA DISPONÍVEIS

Esta seção descreve como instalar todas as atualizações de segurança disponíveis para um host.

Procedimento

1. Para instalar todas as atualizações de segurança, entre:

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

   Note que sem o parâmetro **--security**, **yum** instala atualizações também que incluem correções e melhorias de bugs.

2. Pressione **y** para confirmar, e inicie a instalação:

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

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

3. Opcionalmente, liste os processos que precisam ser reiniciados manualmente após a instalação dos pacotes atualizados:

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

Recursos adicionais

- Seção 4.1, “Mostrar quais serviços precisam ser reiniciados após a aplicação de atualizações de segurança”

3.2. INSTALAÇÃO DE UMA ATUALIZAÇÃO DE SEGURANÇA FORNECIDA POR UMA CONSULTORIA ESPECÍFICA

Em certas situações, por exemplo, se um serviço específico pode ser atualizado sem agendar uma parada, os administradores querem instalar apenas atualizações de segurança para este serviço, e instalar todas as outras atualizações de segurança posteriormente.

Esta seção explica como instalar os pacotes atualizados fornecidos por uma consultoria específica de segurança.

Pré-requisitos

Pré-requisitos

- Uma assinatura válida da Red Hat é atribuída ao anfitrião.
- A identificação da assessoria de segurança é conhecida. Para obter detalhes sobre a exibição das atualizações de segurança instaladas e disponíveis para o host, consulte Capítulo 1, *Identificação de atualizações de segurança*.

Procedimento

1. Instalar as atualizações de segurança fornecidas por uma consultoria específica de segurança. Por exemplo, para instalar as atualizações fornecidas pela consultoria **RHSA-2019:0997**, entre:

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

2. Pressione **y** para confirmar, e inicie a instalação:

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

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

3. Opcionalmente, liste os processos que precisam ser reiniciados manualmente após a instalação dos pacotes atualizados:

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

Recursos adicionais

- Seção 4.1, “Mostrar quais serviços precisam ser reiniciados após a aplicação de atualizações de segurança”

CAPÍTULO 4. TAREFAS ADICIONAIS APÓS A APLICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA

Após ter instalado as atualizações de segurança no Red Hat Enterprise Linux 8, você pode precisar realizar tarefas adicionais. Esta seção descreve estas tarefas.

4.1. MOSTRAR QUAIS SERVIÇOS PRECISAM SER REINICIADOS APÓS A APLICAÇÃO DE ATUALIZAÇÕES DE SEGURANÇA

Quando você atualiza um pacote no Red Hat Enterprise Linux 8, certos processos usando bibliotecas e executáveis atualizados podem precisar ser reiniciados manualmente. Esta seção explica como identificar estes processos.

Pré-requisitos

- As atualizações do Red Hat Enterprise Linux 8 foram instaladas. Para detalhes, veja Capítulo 3, *Instalando atualizações de segurança*.

Procedimento

1. Relacionar todos os processos que ainda utilizam bibliotecas ou executáveis desde o momento anterior à atualização:

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

   O comando **yum needs-restarting** lista apenas processos, não serviços. Isto significa que você não pode reiniciar todos os processos listados usando o utilitário **systemctl**. Por exemplo, o processo **bash** na saída será encerrado quando o usuário proprietário deste processo fizer o logout.