Red Hat Insights 2020-04

Remediating Security Exposures Using the Vulnerability Service and Ansible Playbooks

Automate the Remediation of CVE Security Vulnerabilities in RHEL Environments

Last Updated: 2020-08-18

Red Hat Insights 2020-04 Remediating Security Exposures Using the Vulnerability Service and Ansible Playbooks

Automate the Remediation of CVE Security Vulnerabilities in RHEL Environments

Legal Notice

Abstract

Remediate CVE security vulnerabilities in RHEL environments using the Vulnerability service. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.

Table of Contents

CHAPTER 1. CREATING ANSIBLE PLAYBOOKS TO REMEDIATE CVE EXPOSURES ON RHEL SYSTEMS

The following documentation guides Vulnerability service users in creating Ansible Playbooks to automate the remediation of CVEs on RHEL systems.

Vulnerability service users have two approaches they can use in selecting issues for remediation.

- Remediate multiple CVEs that affect a single system.
- Remediate multiple systems affected by a single CVE.

CHAPTER 2. REMEDIATING MULTIPLE CVES AFFECTING A SINGLE SYSTEM

To remediate CVE exposures on a single system, complete the following steps:

Procedure

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Search for a system by name or scroll through the list to locate the system you wish to remediate.
3. Click on the system name to view system details and list of CVE exposures.
4. Using the checkboxes to the left of the CVE name, select CVEs to remediate on this system and click **Remediate**.
5. Select whether to add the remediations to an **Existing Playbook** (and select the desired playbook from the dropdown list), or click **Create new Playbook** by providing a Playbook Name, then click **Next**.
6. Verify that the information in the Remediation Summary is correct, toggle **Auto Reboot** if available and desired, then click **Create Playbook**.
7. Locate your playbook in Remediations and download the yaml file.
8. Add the yaml file to your Ansible workflow.

CHAPTER 3. REMEDIATING MULTIPLE SYSTEMS AFFECTED BY A SINGLE CVE

To remediate systems of a single CVE exposure, complete the following steps:

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Click on a CVE to view more information about the individual CVE and scroll down to view all exposed systems.
3. Select systems to remediate and click **Remediate**.
4. Select whether to add the remediations to an **Existing Playbook** (and select the desired playbook from the dropdown list), or click **Create new Playbook** by providing a Playbook Name, then click **Next**.
5. Verify that the information in the Remediation Summary is correct, toggle **Auto Reboot** if available and desired, then click **Create Playbook**.
6. Locate your playbook in Remediations and download the yaml file.
7. Add the yaml file to your Ansible workflow.

CHAPTER 4. REFERENCE MATERIALS

To learn more about the Red Hat Insights service, or the other {GUIName_short}, the following resources might also be of interest:

Documentation

- *Assessing and Monitoring Vulnerabilities on RHEL Systems*
- *Generating Vulnerability Reports*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page

CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the **Advisor** service. The *rules* that have always been the currency of Insights are now called Advisor **Recommendations**.

Insights security rules have moved

The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- **Advisor.** Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.
- **Vulnerability.** Assess and monitor the exposure of your RHEL environment to CVEs and security rules.
- **Compliance.** Assess and monitor the compliance of your RHEL systems with SCAP security policies.
- **Patch.** Enable consistent patch workflows for RHEL systems across the open hybrid cloud.
- **Drift.** Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.
- **Policies.** Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- **Inventory.** Topological inventory of RHEL systems under Red Hat Insights management
- **Remediations.** Repository of Ansible Playbooks that you create and manage using Red Hat Insights
- **Subscription Watch.** Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments

Resources

- Red Hat Insights Product Support page
- Red Hat Insights Documentation
- Red Hat Insights Release Notes
- Red Hat Insights blog channel