Red Hat Insights 2021

Remediating Security Exposures Using the Vulnerability Service and Ansible Playbooks

Automate the Remediation of CVE Security Vulnerabilities in RHEL Environments

Last Updated: 2021-09-13

Red Hat Insights 2021 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.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use **Documentation**.
3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click **Submit Bug**.

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.

There are two approaches that vulnerability service users can use, when selecting issues for remediation.

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

2. REMEDIATING MULTIPLE CVES AFFECTING A SINGLE SYSTEM

Complete the following steps to remediate CVE exposures on a single system.

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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 repair on this system and click **Remediate**.
5. Select **Add to existing playbook** or **Create new playbook** and provide a name, depending on your preference. Click **Next**.
6. Verify that the information in the Remediation review is correct. By default, **autoreboot** is enabled. You may click on **Turn off autoreboot** if desired, then click **Submit**.
7. Locate your playbook in Remediations and download the yaml file.
8. Add the yaml file to your Ansible workflow.

3. REMEDIATING MULTIPLE SYSTEMS AFFECTED BY A SINGLE CVE

Complete the following steps, to remediate systems of a single CVE exposure.

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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 **Add to existing playbook** or **Create new playbook** and provide a name, depending on your preference. Click **Next**.
5. Verify that the information in the Remediation review is correct. By default, **autoreboot** is enabled. You may click on **Turn off autoreboot** if desired, then click **Submit**.
6. Locate your playbook in Remediations and download the yaml file.
7. Add the yaml file to your Ansible workflow.

4. REFERENCE MATERIALS

To learn more about the vulnerability service, or the other Insights for Red Hat Enterprise Linux services, the following resources might also be of interest:

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