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: 2021-04-22
Automate the Remediation of CVE Security Vulnerabilities in RHEL Environments
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

1. CREATING ANSIBLE PLAYBOOKS TO REMEDIATE CVE EXPOSURES ON RHEL SYSTEMS ............ 2  
2. REMEDIATING MULTIPLE CVES AFFECTING A SINGLE SYSTEM ........................................ 2  
3. REMEDIATING MULTIPLE SYSTEMS AFFECTED BY A SINGLE CVE .................................. 2  
4. REFERENCE MATERIALS .................................................................................................. 3
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.

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 Insights > 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 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.

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 Insights > 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 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.

4. REFERENCE MATERIALS

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

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