



Red Hat Insights 2021

Remediating Security Exposures Using the Vulnerability Service and Ansible Playbooks

Automate the Remediation of CVE Security Vulnerabilities in RHEL Environments

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

Copyright © 2021 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Remediate CVE security vulnerabilities in RHEL environments using the vulnerability service.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION	4
1. CREATING ANSIBLE PLAYBOOKS TO REMEDIATE CVE EXPOSURES ON RHEL SYSTEMS	4
2. REMEDIATING MULTIPLE CVES AFFECTING A SINGLE SYSTEM	4
3. REMEDIATING MULTIPLE SYSTEMS AFFECTED BY A SINGLE CVE	4
4. REFERENCE MATERIALS	5

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](#)