Managing Security with Red Hat Enterprise Linux Environments

Mohit Goyal
Sr. Principal Product Manager
May 2019
Agenda

Context & what’s happening in the market?  
5 mins

Red Hat Smart Management  
5 mins

Review of Vulnerability & Compliance App within Cloud Services for RHEL  
10 mins

Demo  
10 mins

Discussion & future use cases  
15 mins
The security landscape is changing
Data breaches steadily increasing year over year. 2017 set a record!!

By this count, the number of significant breaches topped 1,300 last year, versus fewer than 200 in 2005

Number of data breaches & records exposed is increasing
Regulations and penalties are on the rise
CHALLENGES COMPLIANCE OFFICERS EXPECT IN 2018

Figure 22: The greatest compliance challenges I expect to face in 2018 is/are:

- Customer due diligence
- Regulatory and political uncertainty
- MiFID II/R
- Vendor compliance
- Sanctions compliance
- Senior management accountability
- Greater clarity on regulations
- Enforcement actions
- Training staff
- Corporate governance
- Global reach and consistency
- Culture
- Data privacy and GDPR
- Data protection
- Continuing regulatory change
- Enhanced monitoring and reporting requirements
- Adequacy and availability of skilled resources
- Implementation of regulatory change
- Coping with limited budget and resources

Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018
What product that will help w/ managing security of Red Hat Enterprise Linux?
Red Hat Smart Management helps organizations optimize and manage their Red Hat Enterprise Linux environments, securing the foundation of their IT infrastructure.
Offering Red Hat Management on-premises or in the cloud to best meet your needs
RED HAT SMART MANAGEMENT
Offering Red Hat Management on-premises or in the cloud to best meet your needs

CLOUD MANAGEMENT SERVICES FOR RHEL

RED HAT SATELLITE

Manage your entire Red Hat environment, connected to the internet or in an airgap environment, including:
- System patching
- Provisioning
- Subscription management

VULNERABILITY

Assess & monitor known security exposures for RHEL
Report findings to stakeholders
Remediate CVEs via Ansible Automation

COMPLIANCE

Assess & monitor compliance to security policies via OpenSCAP
Report findings to stakeholders
Remediate non-compliance issues via Ansible Automation

SYSTEM COMPARISON

Compare system configuration of one host to other hosts
Report findings to stakeholders

#redhat #rhsummit
CLOUD MANAGEMENT SERVICES FOR RED HAT ENTERPRISE LINUX

- Cloud-based management of Red Hat Enterprise Linux hosts
- Managing instances on-premise and in multi-cloud environments
- Focusing on the functionality that customers need
- Offering key benefits of Software-as-a-Service
Software as a Service

Benefits to the Customer

- No infrastructure to maintain
- Register Once
- Easy Setup
- Always on the latest version

Easier to access and scale capabilities
Vulnerability

CLOUD MANAGEMENT SERVICES FOR RED HAT ENTERPRISE LINUX
VULNERABILITY

Remediate all Common Vulnerabilities and Exposures (CVEs) with errata

VULNERABILITY OFFERS

Assess and monitor the risk of vulnerabilities that impact Red Hat products with operational ease

Remediate known Common Vulnerabilities and Exposures (CVEs)

Ability to generate JavaScript Object Notation and CSV view-based reports to keep relevant stakeholders informed
What use cases are addressed for the initial release?

- **Assess/monitor** security (CVEs) exposure level for Red Hat Environment
  - High-level tracking of # vulnerabilities via CVEs, scores, etc.
  - Ability to set “status” for CVE+Host combination
- Creation of Ansible playbooks for remediation
- View-based **reporting** capabilities (JSON, CSV)
  - Ability to Opt-Out a Host for Vulnerability reporting
- Public REST APIs
BUT... INSIGHTS DOES THIS ALREADY, RIGHT?

Vulnerability is security focused—all CVEs with errata

**Red Hat Insights**

- Keep in mind Insights covers availability, performance, security, and stability
- Insights covers ~50 high impact CVEs

**Vulnerability**

- Vulnerability looks at all CVEs that has an errata. Currently ~19,500 CVEs
- Vulnerability uses Common Vulnerability Scoring System (CVSS) to sort risks
Compliance

CLOUD MANAGEMENT SERVICES FOR RED HAT ENTERPRISE LINUX
COMPLIANCE
Built on OpenSCAP reporting

Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease

Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance

Ability to generate JavaScript Object Notation and CSV view-based reports to keep relevant stakeholders informed
Demo
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>CVSS Score</th>
<th>Systems Exposed</th>
<th>Publish Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-3845</td>
<td>A lack of access control was found in the message queues maintained by Satellite's QPID broker and used by katello-agent. A malicious user authenticated to a host registered to Satellite (or Capsule)...</td>
<td>8.0</td>
<td>17</td>
<td>08 Apr 2021</td>
</tr>
<tr>
<td>CVE-2019-0211</td>
<td>A flaw was found in Apache where code executing in a less-privileged child process or thread could execute arbitrary code with the privilege of the parent process (usually root). An attacker having a...</td>
<td>8.8</td>
<td>2</td>
<td>31 Mar 2021</td>
</tr>
<tr>
<td><strong>RESERVED</strong></td>
<td><strong>RESERVED</strong> This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the problem has been announced, the candidate number will be released for publication.</td>
<td>8.8</td>
<td>35</td>
<td>21 Mar 2021</td>
</tr>
</tbody>
</table>
### Vulnerability

#### CVEs

<table>
<thead>
<tr>
<th>CVE Number</th>
<th>Description</th>
<th>CVSS Base Score</th>
<th>Systems Exposed</th>
<th>Publish Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-3883</td>
<td><strong>RESERVED</strong> This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this...</td>
<td>5.3</td>
<td>0</td>
<td>11 Apr 2019</td>
</tr>
<tr>
<td>CVE-2019-9496</td>
<td><strong>RESERVED</strong> This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this...</td>
<td>6.5</td>
<td>0</td>
<td>09 Apr 2019</td>
</tr>
<tr>
<td>CVE-2013-0001</td>
<td>Some details about this vulnerability still need to be determined.</td>
<td>5.5</td>
<td>0</td>
<td>03 Apr 2013</td>
</tr>
<tr>
<td>CVE-2012-0002</td>
<td>Further details about this vulnerability still need to be determined.</td>
<td>7.0</td>
<td>0</td>
<td>02 Apr 2012</td>
</tr>
</tbody>
</table>

#### Systems

- **Red Hat Enterprise Linux management services**

---

**Note:**
- CVSS Base Score: All
- Hide CVEs that do not affect my inventory
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>CVSS Base Score</th>
<th>Systems Exposed</th>
<th>Publish Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-7750</td>
<td>It was found that when acting as an SSH server, paramiko did not properly check whether authentication is completed before processing other requests. A customized SSH client could use this to bypass ...</td>
<td>9.8</td>
<td>13</td>
<td>12 Mar 2018</td>
</tr>
<tr>
<td>CVE-2017-12629</td>
<td>It was found that Apache Lucene would accept an object from an unauthenticated user that could be manipulated through subsequent post requests. An attacker could use this flaw to assemble an object t...</td>
<td>9.8</td>
<td>1</td>
<td>11 Oct 2017</td>
</tr>
<tr>
<td>CVE-2019</td>
<td></td>
<td>8.8</td>
<td>20</td>
<td>26 Nov 2019</td>
</tr>
</tbody>
</table>
CVE-2018-7750

Publish Date: 12 Mar 2018

It was found that when acting as an SSH server, paramiko did not properly check whether authentication is completed before processing other requests. A customized SSH client could use this to bypass authentication when accessing any resources controlled by paramiko.

- Red Hat CVE Database
- MITRE Database

9.8 CVSS Base Score

Severity

Critical

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical impact.
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>rhel6-box</td>
<td>Not Reviewed</td>
<td>3/31/2019, 2:14:07 AM</td>
</tr>
<tr>
<td>ip-172-31-4-98.us-west-2.compute.internal</td>
<td>Not Reviewed</td>
<td>3/22/2019, 5:17:46 PM</td>
</tr>
</tbody>
</table>
**Vulnerability**  >  **CVE-2018-7750**

**CVE-2018-7750**

**Publish Date:** 12 Mar 2018

It was found that when acting as an SSH server, paramiko did not properly check whether authentication is completed before processing other requests. A customized SSH client could use this to bypass authentication when accessing any resources controlled by paramiko.

- Red Hat CVE Database
- MITRE Database

---

<table>
<thead>
<tr>
<th>Find a system by UUID</th>
<th>Remediate with Ansible</th>
</tr>
</thead>
</table>

1 - 13 of 13 items  

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Last Seen</th>
</tr>
</thead>
</table>

**9.8 CVSS Base Score**

**Severity**

![Critical](https://example.com/critical.png)

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical impact.
Remediate with Ansible

Do you want to modify an existing Playbook or create a new one?

- Existing Playbook: dnsmasq
- New Playbook

Playbook Name:

CVE-2018-7750_fix
### Remediate with Ansible

Remediation summary

<table>
<thead>
<tr>
<th>Action</th>
<th>Resolution</th>
<th>Reboot Required</th>
<th>Systems</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-7750</td>
<td>Upgrade packages affected by CVE-2018-7750</td>
<td>true</td>
<td>13</td>
<td>Vulnerability</td>
</tr>
</tbody>
</table>

System reboot is required

- [ ] Auto Reboot

[Create Playbook]
CPE-2018-7750
Publish Date: 12 Mar 2018

It was found that when acting as an SSH server, paramiko did not properly check whether authentication is completed before processing other requests. A customized SSH client could use this to bypass authentication when accessing any resources controlled by paramiko.

- Red Hat CVE Database
- MITRE Database

CVSS Base Score

9.8

Critical

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical impact.
## Systems Reboot

<table>
<thead>
<tr>
<th>Action</th>
<th>Count</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No reboot</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Reboot Required</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Auto Reboot</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Playbook Details
- **Created By:** John Spinks
- **Created:** a few seconds ago
- **Last Modified By:** John Spinks
- **Last Modified:** a few seconds ago

## Search Actions

###CVE-2018-7750
- Upgrade packages affected by CVE-2018-7750
  - Reboot Required: ✔️
  - Systems: 13
  - Type: Vulnerability

---

**Notes:**
- Use the search function to find specific actions.
- Reboot required for 13 systems.
Playbook: CVE-2018-7750_fix

Systems Reboot

- 0 No reboot
- 13 Reboot Required
- Auto Reboot

Playbook Details
Created By: John Spinks
Created: a few seconds ago
Last Modified By: John Spinks
Last Modified: a few seconds ago

CVE-2018-7750
Upgrade packages affected by CVE-2018-7750

- ansible.dgross.redhat.com
- drone67.usersys.redhat.com
- ip-172-31-12-185.us-west-2.compute.internal
## Systems

<table>
<thead>
<tr>
<th>Name</th>
<th>CVEs</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>r7ose01.lnx.aaxc.org</td>
<td>0</td>
<td>4/14/2019, 1:04:08 AM</td>
</tr>
<tr>
<td>dell-r530-44.gsslab.png2.redhat.com</td>
<td>0</td>
<td>4/14/2019, 5:13:36 PM</td>
</tr>
<tr>
<td>ocpnode1.lnx.aaxc.org</td>
<td>0</td>
<td>4/13/2019, 9:43:51 PM</td>
</tr>
<tr>
<td>core-i7.crazy.lab</td>
<td>15</td>
<td>3/18/2019, 5:41:17 AM</td>
</tr>
<tr>
<td>eco6home</td>
<td>0</td>
<td>4/9/2019, 2:45:08 AM</td>
</tr>
</tbody>
</table>
**ic7.example.com**

Hostname: ic7.example.com

UUID: a9cdef1f-4332-4536-a716-ee669840badc

Operating system:

<table>
<thead>
<tr>
<th>CVE</th>
<th>Name</th>
<th>Description</th>
<th>CVSS Base</th>
<th>Status</th>
<th>Publish Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-3863</td>
<td>A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as...</td>
<td>7.5</td>
<td>Not Reviewed</td>
<td>12 Mar 2019</td>
<td></td>
</tr>
<tr>
<td>CVE-2019-3855</td>
<td>An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 in the way packets are read from the</td>
<td>7.5</td>
<td>Not Reviewed</td>
<td>12 Mar 2019</td>
<td></td>
</tr>
</tbody>
</table>
Update the status for this CVE and system

Status:
- Not Reviewed

[Cancel] [Confirm]
Update the status for this CVE and system

Status:
- Not Reviewed
- In-Review
- On-Hold
- Scheduled for Patch
- Resolved
- No Action – Risk Accepted
- Resolved via Mitigation (e.g. done without deploying a patch)
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL76.biucltkfryzubfm0nezhnxwtdh.parx.internal.cloudapp.net</td>
<td>On-Hold</td>
<td>4/12/2019, 3:21:14 PM</td>
</tr>
<tr>
<td>rhel7aws</td>
<td>Scheduled for Patch</td>
<td>4/12/2019, 6:33:40 PM</td>
</tr>
<tr>
<td>rhel7desktop</td>
<td>In-Review</td>
<td>4/12/2019, 6:16:57 PM</td>
</tr>
<tr>
<td>123.45.67.89 (Virtual Machine)</td>
<td>Completed</td>
<td>4/12/2019, 6:16:57 PM</td>
</tr>
</tbody>
</table>
Compliance

External Policy
Standard System Security Profile for R...

11 of 11
Systems above compliance threshold

100%
Systems above threshold

More details
Standard System Security Profile for Red Hat Enterprise Linux 7

Description

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the scap-security-guide package which is developed at

Read more

Minimum threshold for compliance

95%
Standard System Security Profile for Red Hat Enterprise Linux 7

Description

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the scap-security-guide package which is developed at

Read more

Minimum threshold for compliance

95%

<table>
<thead>
<tr>
<th>Name</th>
<th>Profile</th>
<th>Rules Failed</th>
<th>Compliance Score</th>
<th>Last Scanned</th>
</tr>
</thead>
<tbody>
<tr>
<td>ic9.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>✔️ 96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic8.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>✔️ 96.88%</td>
<td>2 months ago</td>
</tr>
</tbody>
</table>
Update compliance threshold

The compliance threshold defines what percentage of rules must be met in order for a system to be determined "compliant"

Compliance threshold (%): 95

Options: Cancel, Save
<table>
<thead>
<tr>
<th>Name</th>
<th>Profile</th>
<th>Rules Failed</th>
<th>Compliance Score</th>
<th>Last Scanned</th>
</tr>
</thead>
<tbody>
<tr>
<td>ic9.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic8.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic6.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic5.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>34</td>
<td>96.69%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic7.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic4.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic3.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>32</td>
<td>96.88%</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ic2.example.com</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>34</td>
<td>96.69%</td>
<td>2 months ago</td>
</tr>
</tbody>
</table>
ic9.example.com

Hostname: ic9.example.com
UUID: ee814b42-2dd9-421e-9848-8b1eb73ba1c5
Operating system:

### External Policy

- **Compliant**
- 995 of 1027 rules passed
- Profile: xccdf_org.ssgproject.content_profile_stand...
- Last scanned: 2019-02-05 19:16:03 UTC

<table>
<thead>
<tr>
<th>Rule</th>
<th>Policy</th>
<th>Severity</th>
<th>Passed</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use direct-ivm with the Device Mapper Storage Driver</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Low</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
ic9.example.com

Hostname: ic9.example.com
UUID: ee814b42-2dd9-421e-9848-8b1eb73ba1c5
Operating system:

External Policy

Compliant
995 of 1027 rules passed
Profile
xccdf_org.ssgproject.content_profile_stand...

Last scanned: 2019-02-05 19:16:03 UTC
<table>
<thead>
<tr>
<th>Rule</th>
<th>Policy</th>
<th>Severity</th>
<th>Passed</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidance Does Not Meet this Requirement Due to Impracticality or Scope</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Low</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Ensure /var/log/audit Located On Separate Partition</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Low</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Verify and Correct File Permissions with RPM</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Ensure Software Patches Installed</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Prevent Log In to Accounts With Empty Password</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
## Compliance

<table>
<thead>
<tr>
<th>Rule</th>
<th>Policy</th>
<th>Severity</th>
<th>Passed</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidance Does Not Meet this Requirement Due to Impracticality or Scope</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Low</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
<tr>
<td>Ensure /var/log/audit Located On Separate Partition</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Low</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
<tr>
<td>Ensure /var/log Located On Separate Partition</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>Unknown</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
<tr>
<td>Verify and Correct File Permissions with RPM</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
<tr>
<td>Ensure Software Patches Installed</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
<tr>
<td>Prevent Log In to Accounts With Empty Password</td>
<td>Standard System Security Profile for Red Hat Enterprise Linux 7</td>
<td>High</td>
<td>1</td>
<td>![Remediation Icon]</td>
</tr>
</tbody>
</table>
ic9.example.com

Hostname: ic9.example.com
UUID: ee814b42-2dd9-421e-9848-8b1eb73ba1c5
Operating system:

External Policy

Compliant
995 of 1027 rules passed
Profile
xccdf_org.ssgproject.content_profile_standard...

Last scanned: 2019-02-05 19:16:03 UTC

Remediation with Ansible
Discussion & Future Use Cases
Discussion

- Do you see value in what you see and will you use it?
- What personas do you expect to use these services?
- What use cases would you like to see addressed?
Customer Engagement & Feedback

- Want to participate in a pilot and provide feedback?
- Have use cases you’d like to see incorporated?
- Mohit Goyal (Product Manager)
  - mgoyal@redhat.com
THANK YOU

linkedin.com/company/Red-Hat

facebook.com/RedHatInc

youtube.com/user/RedHatVideos

twitter.com/RedHat