



CVE

# About cookies on this site



A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

VEX [↗](#)  
Public or  
Last mo

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.



In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for

**Accept Default**

**Do Not Sell or Share My Personal Information**

Description	Statement	Additional information	Affected Packages	CVSS Score Details	Weakness (CWE)	Acknowledgements	FAQ
-------------	-----------	------------------------	-------------------	--------------------	----------------	------------------	-----

## Description

A container privilege escalation flaw was found in certain Red Hat Process Automation Manager images. This issue stems from the `/etc/passwd` file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the `/etc/passwd` file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.

## Statement

Red Hat Product Security has rated this vulnerability as moderate severity for affected products which run on OpenShift. The vulnerability allows for potential privilege escalation within a container, but OpenShift's default, multi-layered security posture effectively mitigates this risk.

The primary controls include the default Security Context Constraints (SCC), which severely limit a container's permissions from the start, and SELinux, which enforces mandatory access control to ensure strict isolation. While other container runtime environments may have different controls available and require case-by-case analysis, OpenShift's built-in defenses are designed to prevent this type of attack.

Out of Box RHEL configuration isolates a single process inside a container. Unless multiple processes are packaged inside a single container, that defeats the principle behind containerization, this bug can not be used to meaningfully escalate privileges.

Also, RHEL, and any common linux distributions do NOT add any additional users to the root group. The presence of the root group is strictly due to conformance with POSIX permission management requirements and can be considered to be an artifact of filesystem permission limitations.

## Additional information

- Bugzilla 2394419: rhpam: privilege escalation via excessive /etc/passwd permissions
- CWE-276: Incorrect Default Permissions

### External references

- <https://www.cve.org/CVERecord?id=CVE-2025-58713>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-58713>

## Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by:

[Clear all](#)

---

<b>Products / Services</b>	Red Hat Process Automation 7
<b>Components</b>	rhpan-businesscentral-monitoring-rhel8
<b>State</b>	Under investigation
<b>Justification</b>	None
<b>Errata</b>	
<b>Release Date</b>	

---

<b>Products / Services</b>	Red Hat Process Automation 7
<b>Components</b>	rhpan-businesscentral-rhel8
<b>State</b>	Under investigation
<b>Justification</b>	None
<b>Errata</b>	
<b>Release Date</b>	

---

<b>Products / Services</b>	Red Hat Process Automation 7
<b>Components</b>	rhpan-controller-rhel8
<b>State</b>	Under investigation
<b>Justification</b>	None
<b>Errata</b>	

## Common Vulnerability Scoring System (CVSS) Score Details

### Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

### CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
<b>CVSS v3 Base Score</b>	6.4	N/A	N/A
<b>Attack Vector</b>	Local	N/A	N/A
<b>Attack Complexity</b>	High	N/A	N/A
<b>Privileges Required</b>	High	N/A	N/A
<b>User Interaction</b>	None	N/A	N/A
<b>Scope</b>	Unchanged	N/A	N/A
<b>Confidentiality Impact</b>	High	N/A	N/A

	Red Hat	NVD	CVE List
Integrity Impact	High	N/A	N/A
Availability Impact	High	N/A	N/A

## CVSS v3 Vector

Red Hat: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

## Acknowledgements

Red Hat would like to thank Antony Di Scala and Michael Whale for reporting this issue.

## Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors?	▼
My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?	▼
What can I do if my product is listed as "Will not fix"?	▼
What can I do if my product is listed as "Fix deferred"?	▼
What is a mitigation?	▼

I have a Red Hat product but it is not in the above list, is it affected? ▼

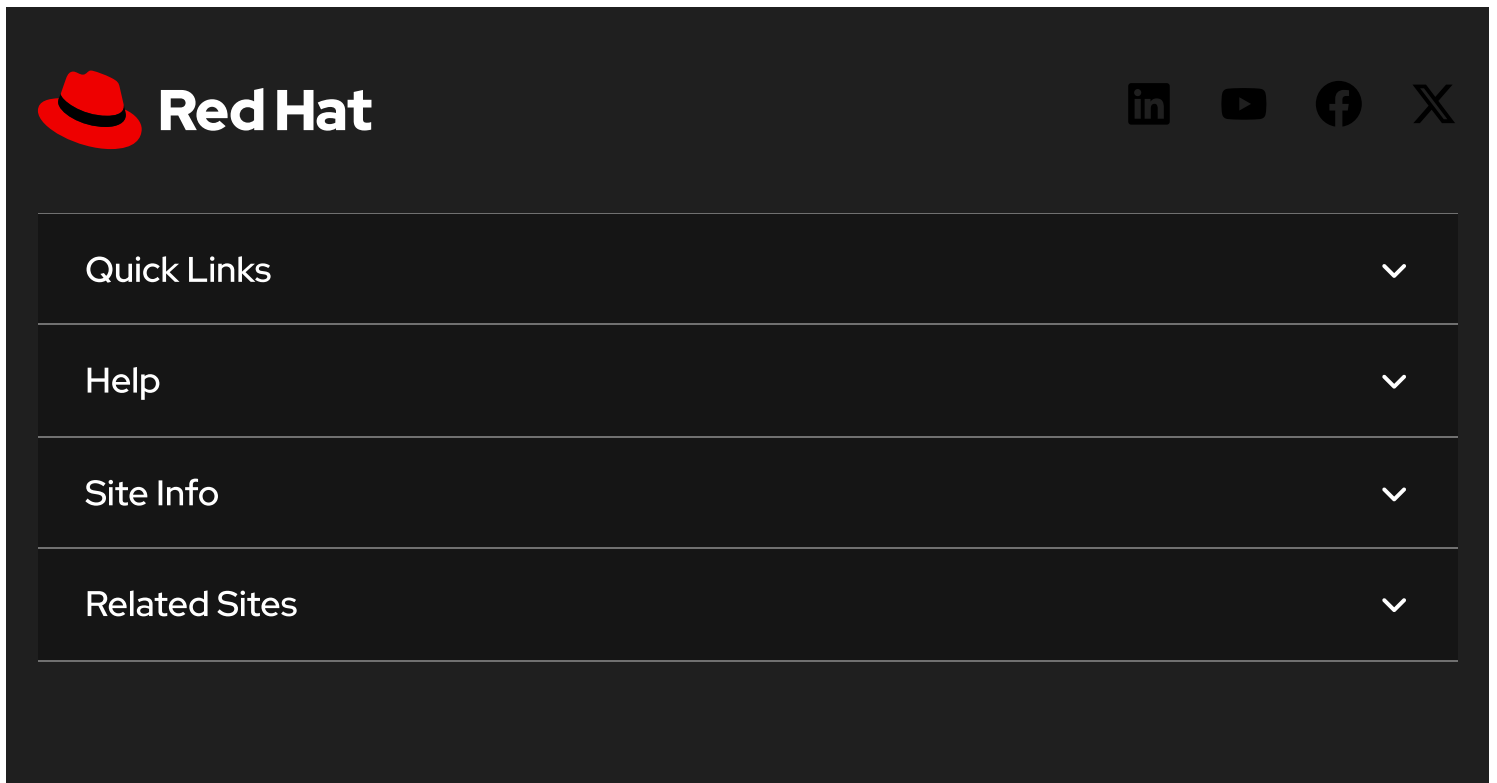
Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected? ▼

Not sure what something means? Check out our [Security Glossary](#).


Want to get errata notifications? Sign up [here](#).

For clarification or corrections, please contact [Red Hat Product Security](#).

Last modified: April 8, 2026 at 1:55:07 PM UTC  
CVE description copyright © 2021



The footer navigation menu is a dark-themed sidebar on the left side of the page. It features the Red Hat logo and name at the top. Below the logo are four menu items: 'Quick Links', 'Help', 'Site Info', and 'Related Sites'. Each item has a white downward-pointing chevron icon to its right. In the top right corner of the footer area, there are four social media icons: LinkedIn, YouTube, Facebook, and X.

 Partial system outage



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

---

[© 2026 Red Hat](#)

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Do Not Sell or Share My Personal Information](#)