



Ansible-automation-platform: privilege escalation via excessive group writable /etc/passwd permissions

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-57847 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-08 14:16:25 UTC |
| Updated | 2026-04-08 21:26:13 UTC |

Description A container privilege escalation flaw was found in certain Ansible Automation Platform images. This issue arises from the /e

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from secalert@redhat.com

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

EPSS: 0.000040000 probability, percentile 0.001470000 (date 2026-04-14)

Problem Types: CWE-276 | CWE-276 Incorrect Default Permissions

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|---------|-------|----------|--|
| 3.1 | secalert@redhat.com | Primary | 6.4 | MEDIUM | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 6.4 | MEDIUM | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------|---------------------------------------|---------------|---------------|
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Ansible Automation Platform 2 | Not specified | Not specified |

References

| Reference | Source | Link | Tags |
|---|---------------------|---|---------------------|
| bugzilla.redhat.com/show_bug.cgi | secalert@redhat.com | bugzilla.redhat.com | |
| access.redhat.com/security/cve/CVE-2025-57847 | secalert@redhat.com | access.redhat.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

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

(en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------|
| CNA | 2025-08-26T17:29:34.376Z | Reported to Red Hat. |
| CNA | 2026-04-08T13:47:09.259Z | Made public. |

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)