



Red Hat Pro

# RHSA-:



2026-05-04

Overview

Updated Pack

## Synopsi:

Important:

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#)

## Topic

An update is now available for Red Hat Ansible Automation Platform 2.5

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## Description

Red Hat Ansible Automation Platform provides an enterprise framework for building, deploying and managing IT automation at scale. IT Managers can provide top-down guidelines on how automation is applied to individual teams, while automation developers retain the freedom to write tasks that leverage existing knowledge without the overhead. Ansible Automation Platform makes it possible for users across an organization to share, vet, and manage automation content by means of a simple, powerful, and agentless language.

Security Fix(es):

- automation-controller: Account hijacking and unauthorized access via unverified email linking (CVE-2026-6266)
- automation-controller: PyJWT accepts unknown `crit` header extensions (RFC 7515 §4.1.11 MUST violation) (CVE-2026-32597)

- automation-controller: denial of service via malformed HTML-like sequences (CVE-2025-69534)
- automation-controller: cryptography Subgroup Attack Due to Missing Subgroup Validation for SECT Curves (CVE-2026-26007)
- automation-gateway: Account hijacking and unauthorized access via unverified email linking (CVE-2026-6266)
- automation-gateway: Rollup: Remote Code Execution via Path Traversal Vulnerability (CVE-2026-27606)
- automation-gateway: SVGGO: Denial of Service via XML entity expansion (CVE-2026-29074)
- automation-gateway: ReDoS via \$data reference (CVE-2025-69873)
- automation-gateway-proxy: Incorrect parsing of IPv6 host literals in net/url (CVE-2026-25679)
- python3.12-django-ansible-base: Account hijacking and unauthorized access via unverified email linking (CVE-2026-6266)
- python3.12-markdown: denial of service via malformed HTML-like sequences (CVE-2025-69534)
- python3.12-jwcrypto: JWCAuto: Memory exhaustion via crafted compressed JWE tokens (CVE-2026-39373)
- python3.12-pyasn1: pyasn1 Vulnerable to Denial of Service via Unbounded Recursion (CVE-2026-30922)
- python3.12-pyasn1: pyasn1: Denial of Service due to memory exhaustion from malformed RELATIVE-OID (CVE-2026-23490)
- python3.12-pyOpenSSL: DTLS cookie callback buffer overflow (CVE-2026-27459)
- receptor: Incorrect parsing of IPv6 host literals in net/url (CVE-2026-25679)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

For details about this release, refer to the release notes listed in the References section.

## Solution

For details on how to apply this update, refer to Ansible Automation Platform documentation.

## Affected Products

- Red Hat Ansible Automation Platform 2.5 for RHEL 9 x86\_64
- Red Hat Ansible Automation Platform 2.5 for RHEL 9 s390x
- Red Hat Ansible Automation Platform 2.5 for RHEL 9 ppc64le
- Red Hat Ansible Automation Platform 2.5 for RHEL 9 aarch64
- Red Hat Ansible Automation Platform 2.5 for RHEL 8 x86\_64
- Red Hat Ansible Automation Platform 2.5 for RHEL 8 s390x
- Red Hat Ansible Automation Platform 2.5 for RHEL 8 ppc64le
- Red Hat Ansible Automation Platform 2.5 for RHEL 8 aarch64
- Red Hat Ansible Inside 1.3 for RHEL 9 x86\_64
- Red Hat Ansible Inside 1.3 for RHEL 9 s390x
- Red Hat Ansible Inside 1.3 for RHEL 9 ppc64le
- Red Hat Ansible Inside 1.3 for RHEL 9 aarch64
- Red Hat Ansible Inside 1.3 for RHEL 8 x86\_64
- Red Hat Ansible Inside 1.3 for RHEL 8 s390x
- Red Hat Ansible Inside 1.3 for RHEL 8 ppc64le
- Red Hat Ansible Inside 1.3 for RHEL 8 aarch64
- Red Hat Ansible Developer 1.2 for RHEL 9 x86\_64
- Red Hat Ansible Developer 1.2 for RHEL 9 s390x
- Red Hat Ansible Developer 1.2 for RHEL 9 ppc64le
- Red Hat Ansible Developer 1.2 for RHEL 9 aarch64
- Red Hat Ansible Developer 1.2 for RHEL 8 x86\_64
- Red Hat Ansible Developer 1.2 for RHEL 8 s390x
- Red Hat Ansible Developer 1.2 for RHEL 8 ppc64le
- Red Hat Ansible Developer 1.2 for RHEL 8 aarch64

## Fixes

- [BZ - 2430472](#) - CVE-2026-23490 pyasn1: pyasn1: Denial of Service due to memory exhaustion from malformed RELATIVE-OID
- [BZ - 2438762](#) - CVE-2026-26007 cryptography: cryptography Subgroup Attack Due to Missing Subgroup Validation for SECT Curves
- [BZ - 2439070](#) - CVE-2025-69873 ajv: ReDoS via \$data reference
- [BZ - 2442530](#) - CVE-2026-27606 rollup: Rollup: Remote Code Execution via Path Traversal Vulnerability
- [BZ - 2444839](#) - CVE-2025-69534 python-markdown: denial of service via malformed HTML-like sequences
- [BZ - 2445132](#) - CVE-2026-29074 svg: SVGO: Denial of Service via XML entity expansion
- [BZ - 2445356](#) - CVE-2026-25679 net/url: Incorrect parsing of IPv6 host literals in net/url
- [BZ - 2447194](#) - CVE-2026-32597 pyjwt: PyJWT accepts unknown `crit` header extensions (RFC 7515 4.1.11 MUST violation)
- [BZ - 2448503](#) - CVE-2026-27459 pyOpenSSL: DTLS cookie callback buffer overflow
- [BZ - 2448553](#) - CVE-2026-30922 pyasn1: pyasn1 Vulnerable to Denial of Service via Unbounded Recursion
- [BZ - 2456187](#) - CVE-2026-39373 JWCrypto: python-cryptography: python: JWCrypto: Memory exhaustion via crafted compressed JWE tokens
- [BZ - 2458142](#) - CVE-2026-6266 aap-controller: aap-gateway: Account hijacking and unauthorized access via unverified email linking

## CVEs

- [CVE-2025-69534](#)
- [CVE-2025-69873](#)
- [CVE-2026-6266](#)
- [CVE-2026-23490](#)
- [CVE-2026-25679](#)
- [CVE-2026-26007](#)
- [CVE-2026-27459](#)
- [CVE-2026-27606](#)
- [CVE-2026-29074](#)
- [CVE-2026-30922](#)
- [CVE-2026-32597](#)
- [CVE-2026-39373](#)

## References

- <https://access.redhat.com/security/updates/classification/#important>
- [https://docs.redhat.com/en/documentation/red\\_hat\\_automation\\_platform/2.5/html/release\\_notes/patch\\_releases](https://docs.redhat.com/en/documentation/red_hat_automation_platform/2.5/html/release_notes/patch_releases)
- [https://docs.redhat.com/en/documentation/red\\_hat\\_automation\\_platform/2.5#Upgrading](https://docs.redhat.com/en/documentation/red_hat_automation_platform/2.5#Upgrading)


---

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.




- [Quick Links](#) 


---

- [Help](#) 


---


- [Site Info](#) 

---

- [Related Sites](#) 

---

 Loading



- [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 Opt-Out Rights](#)