# RHSA-2026:13508 - Security Advisory

发布： 2026-05-04 已更新： 2026-05-04



## 概述

Important: Red Hat Ansible Automation Platform 2.6 Product Security and Bug Fix Update

## 类型/严重性

Security Advisory: Important

**Red Hat Lightspeed patch analysis**

识别并修复受此公告影响的系统。

查看受影响的系统

## 标题

An update is now available for Red Hat Ansible Automation Platform 2.6

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.

## 描述

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: DTLS cookie callback buffer overflow (CVE-2026-27459)

- 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-gateway: Account hijacking and unauthorized access via unverified email linking (CVE-2026-6266)
- automation-gateway-proxy: Incorrect parsing of IPv6 host literals in net/url (CVE-2026-25679)
- automation-platform-ui: Rollup: Remote Code Execution via Path Traversal Vulnerability (CVE-2026-27606)
- automation-platform-ui: minimatch: Denial of Service via specially crafted glob patterns (CVE-2026-26996)
- 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: JWCrypto: 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.

## 解决方案

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

## 受影响的产品

- Red Hat Ansible Automation Platform 2.6 for RHEL 10 x86_64
- Red Hat Ansible Automation Platform 2.6 for RHEL 10 s390x
- Red Hat Ansible Automation Platform 2.6 for RHEL 10 ppc64le
- Red Hat Ansible Automation Platform 2.6 for RHEL 10 aarch64
- Red Hat Ansible Automation Platform 2.6 for RHEL 9 x86_64
- Red Hat Ansible Automation Platform 2.6 for RHEL 9 s390x
- Red Hat Ansible Automation Platform 2.6 for RHEL 9 ppc64le
- Red Hat Ansible Automation Platform 2.6 for RHEL 9 aarch64
- Red Hat Ansible Inside 1.4 x86_64
- Red Hat Ansible Inside 1.4 s390x
- Red Hat Ansible Inside 1.4 ppc64le
- Red Hat Ansible Inside 1.4 aarch64
- Red Hat Ansible Developer 1.3 for RHEL 10 x86_64
- Red Hat Ansible Developer 1.3 for RHEL 10 s390x
- Red Hat Ansible Developer 1.3 for RHEL 10 ppc64le
- Red Hat Ansible Developer 1.3 for RHEL 10 aarch64
- Red Hat Ansible Developer 1.3 for RHEL 9 x86_64
- Red Hat Ansible Developer 1.3 for RHEL 9 s390x
- Red Hat Ansible Developer 1.3 for RHEL 9 ppc64le
- Red Hat Ansible Developer 1.3 for RHEL 9 aarch64

## 修复

- BZ - 2430472 - CVE-2026-23490 pyasn1: pyasn1: Denial of Service due to memory exhaustion from malformed RELATIVE-OID
- BZ - 2436341 - CVE-2025-14550 Django: Django: Denial of Service via crafted request with duplicate headers

- BZ - 2441268 - CVE-2026-26996 minimatch: minimatch: Denial of Service via specially crafted glob patterns
- 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 - 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

## CVE

- CVE-2025-14550
- CVE-2025-69534
- CVE-2026-6266
- CVE-2026-23490
- CVE-2026-25679
- CVE-2026-26996
- CVE-2026-27459
- CVE-2026-27606
- CVE-2026-30922
- CVE-2026-32597
- CVE-2026-39373

## 参考

- https://access.redhat.com/security/updates/classification/#important
- https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.6/html/release_notes/patch_releases
- https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.6#Upgrade

---

Red Hat 安全团队联络方式为 secalert@redhat.com。 更多联络细节请参考 https://access.redhat.com/security/team/contact/。

All systems operational