RHSA-2024:1640 - Security Advisory

Issued: 2024-04-02 Updated: 2024-04-02

Synopsis

Moderate: Red Hat Ansible Automation Platform 2.4 Product Security and Bug Fix Update

Type/Severity

Security Advisory: Moderate

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 2.4

Red Hat Product Security has rated this update as having a security impact of Moderate. 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: Django: denial-of-service in 'intcomma' template filter (CVE-2024-24680)
- automation-controller: aiohttp: http request smuggling (CVE-2024-23829)
- automation-controller: aiohttp: follow_symlinks directory traversal vulnerability (CVE-2024-23334)
- automation-controller: Jinja2: HTML attribute injection when passing user input as keys to xmlattr filter (CVE-2024-22195)
- automation-controller: cryptography: NULL-dereference when loading PKCS7 certificates (CVE-2023-49083)
- automation-controller: aiohttp: numerous issues in HTTP parser with header parsing (CVE-2023-47627)
- automation-controller: Twisted: disordered HTTP pipeline response in twisted.web (CVE-2023-46137)
- automation-controller: axios: exposure of confidential data stored in cookies (CVE-2023-45857)
- automation-controller: GitPython: Blind local file inclusion (CVE-2023-41040)
- python3-aiohttp/python39-aiohttp: http request smuggling (CVE-2024-23829)
- python3-aiohttp/python39-aiohttp: follow_symlinks directory traversal vulnerability (CVE-2024-23334)
- python3-django/python39-django: Potential regular expression denial-of-service in django.utils.text.Truncator.words() (CVE-2024-27351)
- receptor: golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- receptor: golang: net/http/internal: Denial of Service (DoS) via Resource Consumption via HTTP requests (CVE-2023-39326)

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.

Updates and fixes for automation controller:

- Fixed bug where schedule prompted variables and survey answers were reset on edit when changing one of the basic form fields (AAP-20967)
- Fixed the update execution environment image to no longer fail jobs that use the previous image (AAP-21733)
- Removed string validation using comparisons of English literals for comparison, replacing validation with error/op codes as a universal approach to validation and comparison (AAP-21721)
- Fixed dispatcher to appropriately terminate child processes when dispatcher terminates (AAP-21049)
- Fixed upgrade from Ansible Tower 3.8.6 to AAP 2.4 to no longer fail upon database schema migration (AAP-19738)
- automation-controller has been updated to 4.5.5

Updates and fixes for receptor:

- Fixes a receptor dialing issue where the connection attempt is timed out too aggressively (AAP-21838, AAP-21828)
- receptor has been updated to 1.4.5

Additional fixes:

- ansible-core has been updated to 2.15.10
- ansible-runner has been updated to 2.3.6
- python3-aiohttp/python39-aiohttp has been updated to 3.9.3
- python3-django/python39-django has been updated 4.2.11
- python3-pulpcore/python39-pulpcore has been updated 3.28.24

Solution

Red Hat Ansible Automation Platform

Affected Products

- Red Hat Ansible Automation Platform 2.4 for RHEL 9 x86_64
- Red Hat Ansible Automation Platform 2.4 for RHEL 9 s390x
- Red Hat Ansible Automation Platform 2.4 for RHEL 9 ppc64le
- Red Hat Ansible Automation Platform 2.4 for RHEL 9 aarch64
- Red Hat Ansible Automation Platform 2.4 for RHEL 8 x86_64
- Red Hat Ansible Automation Platform 2.4 for RHEL 8 s390x
- Red Hat Ansible Automation Platform 2.4 for RHEL 8 ppc64le
- Red Hat Ansible Automation Platform 2.4 for RHEL 8 aarch64
- Red Hat Ansible Inside 1.2 for RHEL 9 x86_64
- Red Hat Ansible Inside 1.2 for RHEL 9 s390x
- Red Hat Ansible Inside 1.2 for RHEL 9 ppc64le

- Red Hat Ansible Inside 1.2 for RHEL 9 aarch64
- Red Hat Ansible Inside 1.2 for RHEL 8 x86_64
- Red Hat Ansible Inside 1.2 for RHEL 8 s390x
- Red Hat Ansible Inside 1.2 for RHEL 8 ppc64le
- Red Hat Ansible Inside 1.2 for RHEL 8 aarch64
- Red Hat Ansible Developer 1.1 for RHEL 9 x86_64
- Red Hat Ansible Developer 1.1 for RHEL 9 s390x
- Red Hat Ansible Developer 1.1 for RHEL 9 ppc64le
- Red Hat Ansible Developer 1.1 for RHEL 9 aarch64
- Red Hat Ansible Developer 1.1 for RHEL 8 x86_64
- Red Hat Ansible Developer 1.1 for RHEL 8 s390x
- Red Hat Ansible Developer 1.1 for RHEL 8 ppc64le
- Red Hat Ansible Developer 1.1 for RHEL 8 aarch64

Fixes

- BZ - 2246264 - CVE-2023-46137 python-twisted: disordered HTTP pipeline response in twisted.web
- BZ - 2247040 - CVE-2023-41040 GitPython: Blind local file inclusion
- BZ - 2248979 - CVE-2023-45857 axios: exposure of confidential data stored in cookies
- BZ - 2249825 - CVE-2023-47627 python-aiohttp: numerous issues in HTTP parser with header parsing
- BZ - 2253330 - CVE-2023-39326 golang: net/http/internal: Denial of Service (DoS) via Resource Consumption via HTTP requests
- BZ - 2255331 - CVE-2023-49083 python-cryptography: NULL-dereference when loading PKCS7 certificates
- BZ - 2257854 - CVE-2024-22195 jinja2: HTML attribute injection when passing user input as keys to xmlattr filter
- BZ - 2261856 - CVE-2024-24680 Django: denial-of-service in ``intcomma`` template filter
- BZ - 2261887 - CVE-2024-23334 aiohttp: follow_symlinks directory traversal vulnerability
- BZ - 2261909 - CVE-2024-23829 python-aiohttp: http request smuggling
- BZ - 2262921 - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads
- BZ - 2266045 - CVE-2024-27351 python-django: Potential regular expression denial-of-service in django.utils.text.Truncator.words()

CVEs

- CVE-2023-39326
- CVE-2023-41040
- CVE-2023-45857

- CVE-2023-46137
- CVE-2023-47627
- CVE-2023-49083
- CVE-2024-1394
- CVE-2024-22195
- CVE-2024-23334
- CVE-2024-23829
- CVE-2024-24680
- CVE-2024-27351

References

- https://access.redhat.com/security/updates/classification/#moderate

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.