Red Hat P

RHSA

6-03-26

Overview

Updated P

Synop

Importar

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

A new release is now available for Red Hat Satellite 6.17 for RHEL 9.

Description

Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments.

Security Fix(es):

- python-django: Django: SQL Injection via crafted column aliases (CVE-2026-1287)
- python-django: Django: SQL Injection via RasterField band index parameter (CVE-2026-1207)
- python-django: Django: Denial of Service via crafted HTML inputs (CVE-2026-1285)
- python-django: Django: SQL injection via crafted column aliases in QuerySet.order_by() (CVE-2026-1312)
- python-django: Django: Denial of Service via crafted request with duplicate headers (CVE-2025-14550)
- python-brotli: Brotli decompression bomb DoS in scrapy/scrapy (CVE-2025-6176)
- rubygem-foreman_kubevirt: foreman_kubevirt: Man-in-the-Middle due to insecure default SSL verification (CVE-2026-1531)
- rubygem-fog-kubevirt: fog-kubevirt: Man-in-the-Middle vulnerability due to disabled certificate validation (CVE-2026-1530)
- rubygem-rubyipmi: Red Hat Satellite: Remote Code Execution in rubyipmi via malicious BMC username (CVE-2026-0980)
- foreman: Foreman: Remote Code Execution via command injection in WebSocket proxy (CVE-2026-1961)
- yggdrasil-worker-forwarder: Unexpected session resumption in crypto/tls (CVE-2025-68121)
- Katello: Denial of Service and potential information disclosure via SQL injection (CVE-2026-4324)

Bug Fix(es):

- High memory usage of postgres processes on scaled Capsule (SAT-42871)
- AttributeError: 'NoneType' object has no attribute '_artifacts' when running pulpcore-container-handle-image-metadata in the post-upgrade step for Satellite 6.17 (SAT-42873)
- Lifecycle Environment shows 2 Library options (SAT-42881)
- Executing foreman-rake command in the satellite, prints warning "W, [2025-08-28T14:25:04.030121 #11656] WARN -- : Scoped order is ignored, it's forced to be batch order." (SAT-42882)
- Upgrade to Sat 6.16 does not cleanup Postgresql12 which is reported as security risk/vulnerability by the scanners on Sat 6.17 & 6.18. (SAT-43118)

Solution

Before applying this update, make sure all previously released errata
relevant to your system have been applied.

For detailed instructions how to apply this update, refer to:

https://docs.redhat.com/en/documentation/red_hat_satellite/6.17/html/updating_red_hat_satellite/index

Affected Products

- Red Hat Satellite 6.17 x86_64
- Red Hat Satellite Capsule 6.17 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64

Fixes

- BZ - 2408762 - CVE-2025-6176 Scrapy: python-scrapy: brotli: Python brotli decompression bomb DoS
- BZ - 2429874 - CVE-2026-0980 rubyipmi: Red Hat Satellite: Remote Code Execution in rubyipmi via malicious BMC username
- BZ - 2433784 - CVE-2026-1530 fog-kubevirt: fog-kubevirt: Man-in-the-Middle vulnerability due to disabled certificate validation
- BZ - 2433786 - CVE-2026-1531 foreman-kubevirt: foreman_kubevirt: Man-in-the-Middle due to insecure default SSL verification
- BZ - 2436338 - CVE-2026-1207 Django: Django: SQL Injection via RasterField band index parameter
- BZ - 2436339 - CVE-2026-1287 Django: Django: SQL Injection via crafted column aliases
- BZ - 2436340 - CVE-2026-1285 Django: Django: Denial of Service via crafted HTML inputs
- BZ - 2436341 - CVE-2025-14550 Django: Django: Denial of Service via crafted request with duplicate headers
- BZ - 2436342 - CVE-2026-1312 Django: Django: SQL injection via crafted column aliases in QuerySet.order_by()
- BZ - 2437036 - CVE-2026-1961 forman: Foreman: Remote Code Execution via command injection in WebSocket proxy
- BZ - 2437111 - CVE-2025-68121 crypto/tls: Unexpected session resumption in crypto/tls
- BZ - 2448349 - CVE-2026-4324 rubygem-katello: Katello: Denial of Service and potential information disclosure via SQL injection
- SAT-42871 - High memory usage of postgres processes on scaled Capsule [rhn_satellite_6.17]
- SAT-42873 - AttributeError: 'NoneType' object has no attribute '_artifacts' when running pulpcore-container-handle-image-metadata in the post-upgrade step for Satellite 6.17 [rhn_satellite_6.17]
- SAT-42881 - Lifecycle Environment shows 2 Library options [rhn_satellite_6.17]
- SAT-42882 - Executing foreman-rake command in the satellite, prints warning "W, [2025-08-28T14:25:04.030121 #11656] WARN -- : Scoped order is ignored, it's forced to be batch order." [rhn_satellite_6.17]

CVEs

- CVE-2025-6176
- CVE-2025-14550
- CVE-2025-68121

- CVE-2026-0980
- CVE-2026-1207
- CVE-2026-1285
- CVE-2026-1287
- CVE-2026-1312
- CVE-2026-1530
- CVE-2026-1531
- CVE-2026-1961
- CVE-2026-4324

References

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

---

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