Red Hat F

RHSA

Advis

5-03-26

Overview

Updated P

Synop

Importa

Type/

Security

Red H

Identi

View a

Topic

A new release is now available for Red Hat Satellite 6.18 for RHEL 9.

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 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):

- yggdrasil-worker-forwarder: Memory exhaustion in query parameter parsing in net/url (CVE-2025-61726)
- yggdrasil-worker-forwarder: golang: Denial of Service due to excessive resource consumption via crafted certificate (CVE-2025-61729)
- yggdrasil-worker-forwarder: Unexpected session resumption in crypto/tls (CVE-2025-68121)
- rubygem-rubyipmi: Remote Code Execution in rubyipmi via malicious BMC username (CVE-2026-0980)
- rubygem-foreman_kubevirt: foreman_kubevirt: Man-in-the-Middle due to insecure default SSL verification (CVE-2026-1531)
- foreman: Foreman: Remote Code Execution via command injection in WebSocket proxy (CVE-2026-1961)
- rubygem-katello: Katello: Denial of Service and potential information disclosure via SQL injection (CVE-2026-4324)

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://access.redhat.com/documentation/en-us/red_hat_satellite/6.18/html/updating_red_hat_satellite/index

Affected Products

- Red Hat Satellite 6.18 x86_64
- Red Hat Satellite Capsule 6.18 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64

Fixes

- SAT-41530 - Sync all inventory status returns "Cannot read properties of undefined (reading 'sync')" when satellite has iop enabled

- SAT-42707 - AttributeError: 'NoneType' object has no attribute '_artifacts' when running pulpcore-container-handle-image-metadata in the post-upgrade step for Satellite 6.17
- SAT-42708 - Both Recommendations and Vulnerabilities apps don't work when location is set to Any
- SAT-42710 - Lifecycle Environment shows 2 Library options
- SAT-42711 - 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-42712 - High memory usage of postgres processes on scaled Capsule
- SAT-42713 - "Too many open files" error during capsule content consumption (especially Streamed capsules)
- SAT-42714 - IOP-enabled Satellite does not clean up old inventory and client tars in ingress service resulting in disk space growth
- SAT-42715 - IoP detection during app initialization should not rely on possibly stale values
- SAT-42716 - Inconsistent Display of Red Hat LightSpeed Recommendations in Satellite WebUI
- SAT-42717 - SingleHostReportJob fails with undefined method `subtree_ids' for nil:NilClass when host belongs to a hostgroup and value of host_registration_insights_inventory is false
- SAT-42718 - The ForemanInventoryUpload::Async::SingleHostReportJob, job always fails on Satellite 6.18.2 when IoP is enabled
- SAT-43310 - 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-43742 - Navigating from the Recommendations tab to another tab redirects you to the overview tab
- SAT-43743 - Remediation fails for hosts re-registered to Insights after enabling IoP

CVEs

- CVE-2025-61726
- CVE-2025-61729
- CVE-2025-68121
- CVE-2026-0980
- 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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use