



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA Advis

5-03-26

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Updated P

Synop

Importa

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Type/

Security

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Red H

Identifi

View a

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Topic

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy

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: go-lang: 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/>.



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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

All policies and guidelines

Digital accessibility

Cookie Preferences and Opt-Out Rights