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

Red Hat F

RHSA

5-05-14

Overview

Updated P

Synop

Moderat

Type/

Security

Red H

Identi

View a

Topic

Updatec

Red Hat Satellite.

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.

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.

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.

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.

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".

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

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):

- foreman_ygg_worker: net/http: sensitive headers incorrectly sent after cross-domain redirect (CVE-2024-45336)
- foreman_ygg_worker: Golang FIPS zeroed buffer (CVE-2024-9355)
- yggdrasil: net/http: sensitive headers incorrectly sent after cross-domain redirect (CVE-2024-45336)

Users of Red Hat Satellite are advised to upgrade to these updated packages, which fix these bugs.

Solution

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

For details on how to apply this update, refer to:

https://access.redhat.com/documentation/en-us/red_hat_satellite/6.16/html/updating_red_hat_satellite/index

Affected Products

- Red Hat Enterprise Linux for x86_64 10 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64

- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86_64
- Red Hat Enterprise Linux Server - AUS 8.2 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.2 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.8 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.2 x86_64
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64

- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 10.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 9.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 6 for RHEL 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 6 for RHEL 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64

Fixes

- BZ - 2315719 - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer

- BZ - 2341751 - CVE-2024-45336 golang: net/http: net/http: sensitive headers incorrectly sent after cross-domain redirect

CVEs

- CVE-2024-9355
- CVE-2024-45336

References

- https://access.redhat.com/security/updates/classification/#moderate
- https://access.redhat.com/documentation/en-us/red_hat_satellite/6.17/html/updating_red_hat_satellite/index

---

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