



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

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.

5-03-24

Overview

Updated P

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

Synop

Moderat

Accept Default

Do Not Sell or Share My Personal Information

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) ↗

Topic

An update for the redhat-ds:12 module is now available for Red Hat Directory Server 12.2 E4S 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 Directory Server is an LDAPv3-compliant directory server. The suite of packages includes the Lightweight Directory Access Protocol (LDAP) server, as well as command-line utilities and Web UI packages for server administration.

Security Fix(es):

- 389-ds-base: 389-ds-base: Remote Code Execution and Denial of Service via heap buffer overflow (CVE-2025-14905)

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.

Solution


For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 


Affected Products

- Red Hat Directory Server - 4 years of updates 12 for RHEL 9.2 x86_64

Fixes

- BZ - 2423624  - CVE-2025-14905 389-ds-base: 389-ds-base: Remote Code Execution and Denial of Service via heap buffer overflow

CVEs

- CVE-2025-14905 

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/>.



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 Do Not Sell or Share My Personal Information