



Red Hat Product Errata    RHSA-2026:4207 - Security Advisory

# RHSA-2026:4207 - Security Advisory

Issued: 2026-03-10    Updated: 2026-03-10

[Overview](#)[Updated Packages](#)

## Synopsis

Moderate: 389-ds-base security update

## 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 389-ds-base is now available for Red Hat Enterprise Linux 9.6 Extended Update Support.

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

389 Directory Server is an LDAP version 3 (LDAPv3) compliant server. The base packages include the Lightweight Directory Access Protocol (LDAP) server and command-line utilities 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 Enterprise Linux for x86\_64 - Extended Update Support 9.6 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.6 x86\_64
- Red Hat CodeReady Linux Builder for x86\_64 - Extended Update Support 9.6 x86\_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.6 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x

## Fixes

- [BZ - 2423624](#) - CVE-2025-14905 389-ds-base: 389-ds-base: Remote Code Execution and Denial of Service via heap buffer overflow
- [RHEL-140087](#) - Upgrading IDM to latest version: 389-ds-base and ipa-server breaks replication [rhel-9.6.z]

## CVEs

- [CVE-2025-14905](#)

## References

- <https://access.redhat.com/security/updates/classification/#moderate>

The Red Hat security contact is [secalert@redhat.com](mailto: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](#)