



Red Hat Product Errata RHSA-2026:6220 - Security Advisory

RHSA-2026:6220 - Security Advisory

Issued: 2026-03-31 Updated: 2026-03-31

[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 7 Extended Lifecycle 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 Server - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le

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 Opt-Out Rights