



[Red Hat Product Errata](#)    [RHSA-2025:19852 - Security Advisory](#)

# RHSA-2025:19852 - Security Advisory

Issued: 2025-11-06    Updated: 2025-11-06

[Overview](#)

[Updated Packages](#)

## Synopsis

Important: sssd security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for sssd is now available for Red Hat Enterprise Linux 9.4 Extended Update Support.

Red Hat Product Security has rated this update as having a security impact of Important. 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

The System Security Services Daemon (SSSD) service provides a set of daemons to manage access to remote directories and authentication mechanisms. It also provides the Name Service Switch (NSS) and the Pluggable Authentication Modules (PAM) interfaces toward the system, and a pluggable back-end system to connect to multiple different account sources.

Security Fix(es):

- sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems (CVE-2025-11561)

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 9.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.4 x86\_64
- Red Hat CodeReady Linux Builder for x86\_64 - Extended Update Support 9.4 x86\_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x

## Fixes

- BZ - 2402727  - CVE-2025-11561 sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems

## CVEs


- [CVE-2025-11561](#) 

## References


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

---

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat icon) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward-pointing chevron icon on the right: "Quick Links", "Help", "Site Info", and "Related Sites".

 All systems operational



The image shows a dark-themed footer for Red Hat. On the left is a small grey hat icon. To its right are four links: "About Red Hat", "Jobs", "Events", and "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](#)