



Red Hat F

# RHSA Advis



25-11-06

Overview

Updated P

## Synop

Importa

## 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 7 Extended Lifecycle 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 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 - 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/>.



---

Quick Links 


---

Help 


---


Site Info 

---

Related Sites 

---

 All systems operational



[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](#)