CVE-

VEX
Public on
Last modi

Jump to section

Description

A flaw was found in the integration of Active Directory and the System Security Services Daemon (SSSD) on Linux systems. In default configurations, the Kerberos local authentication plugin (sssd_krb5_localauth_plugin) is enabled, but a fallback to the an2ln plugin is possible. This fallback allows an attacker with permission to modify certain AD attributes (such as userPrincipalName or samAccountName) to impersonate privileged users, potentially resulting in unauthorized access or privilege escalation on domain-joined Linux hosts.

Statement

The Red Hat Product Security team has assessed this issue as High severity for domain-joined Linux systems using default SSSD configurations. While the Kerberos local authentication plugin (sssd_krb5_localauth_plugin) is enabled by default, fallback to the an2ln plugin can occur, allowing a domain user who can modify certain Active Directory attributes (such as userPrincipalName or

samAccountName) to map to privileged local accounts. This could lead to unauthorized access or elevated privileges on affected Linux hosts. Administrators are advised to review and apply recommended hardening configurations to mitigate this behavior.

Mitigation

To mitigate this issue, ensure the SSSD Kerberos local authentication plugin (sssd_krb5_localauth_plugin) is configured and the an2ln plugin is disabled by adding "disable = an2ln" in a krb5 include file, for example /var/lib/sss/pubconf/krb5.include.d/localauth_plugin and make sure it is included in the Kerberos configuration. Apply vendor updates and follow Red Hat guidance for SSSD hardening.

Additional information

- Bugzilla 2402727: sssd: SSSD default Kerberos configuration allows privilege escalation on AD-joined Linux systems
- CWE-269: Improper Privilege Management

External references

- https://www.cve.org/CVERecord?id=CVE-2025-11561
- https://nvd.nist.gov/vuln/detail/CVE-2025-11561
- https://blog.async.sg/kerberos-ldr

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata

Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	sssd
State	Fixed

Justification	None
Errata	RHSA-2025:19851
Release Date	November 6, 2025

Products / Services	Red Hat Enterprise Linux 10
Components	sssd
State	Fixed
Justification	None
Errata	RHSA-2025:21020
Release Date	November 11, 2025

Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support

1-10 of 29

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD

	Red Hat	NVD
CVSS v3 Base Score	8.8	N/A
Attack Vector	Network	N/A
Attack Complexity	Low	N/A
Privileges Required	Low	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	N/A
Availability Impact	High	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

Red Hat would like to thank Zavier Lee for reporting this issue.

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors? >
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? >

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: November 4, 2025 at 10:48:45 AM UTC