



# Sssd: out-of-bounds read in the sssd

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-6245
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 19:16:38 UTC
<b>Updated</b>	2026-04-17 15:08:01 UTC
<b>Description</b>	A flaw was found in the System Security Services Daemon (SSSD). The pam_passkey_child_read_data() function within th

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from secalert@redhat.com

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

**EPSS:** 0.000100000 probability, percentile 0.010730000 (date 2026-04-21)

**Problem Types:** CWE-805 | CWE-805 Buffer Access with Incorrect Length Value

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2026-6245">access.redhat.com/security/cve/CVE-2026-6245</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-13T18:53:44.518Z	Reported to Red Hat.
CNA	2026-04-15T18:20:05.454Z	Made public.

### Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

There are currently no legacy QID mappings associated with this CVE.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)