



Bug 2419369 (CVE-2025-14104) - CVE-2025-14104 util-linux: util-linux: Heap buffer overread in setpwnam() when processing 256-byte usernames

Keywords:

Reported: 2025-12-05 14:21 UTC by OSIDB Bzimport

Status: MODIFIED

Modified: 2026-04-07 16:12 UTC ([History](#))

Alias: CVE-2025-14104

CC List: 13 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2419370](#) [2419371](#)

Blocks:


TreeView+ [depends on](#) / [blocked](#)

Attachments [\(Terms of Use\)](#)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2026:2101	0	None	None	None	2026-02-05 13:39:54 UTC
Red Hat Product Errata	RHBA-2026:2102	0	None	None	None	2026-02-05 13:34:49 UTC
Red Hat Product Errata	RHBA-2026:2203	0	None	None	None	2026-02-05 23:06:54 UTC

Red Hat Product Errata	RHBA-2026:2205	0	None	None	None	2026-02-05 23:18:03 UTC
Red Hat Product Errata	RHBA-2026:2260	0	None	None	None	2026-02-09 02:57:59 UTC
Red Hat Product Errata	RHBA-2026:2325	0	None	None	None	2026-02-09 11:43:56 UTC
Red Hat Product Errata	RHBA-2026:2665	0	None	None	None	2026-02-12 15:30:27 UTC
Red Hat Product Errata	RHSA-2026:1696	0	None	None	None	2026-02-02 10:05:18 UTC
Red Hat Product Errata	RHSA-2026:1852	0	None	None	None	2026-02-04 11:05:03 UTC
Red Hat Product Errata	RHSA-2026:1913	0	None	None	None	2026-02-04 19:48:46 UTC

OSIDB Bzimport  2025-12-05 14:21:04 UTC[Description](#)

A flaw was found in util-linux. Heap buffer overread when processing 256-byte usernames. Affects any SUID login-utils utility writing to password database. The setpwnam() function allocates a 256-byte buffer but accesses linebuf[256] when username length equals 256, causing a heap buffer overread.

Karel Zak 2026-01-14 13:10:32 UTC

[Comment 2](#)

Fixed in upstream release v2.41.3, upgrade already available in f44 and f43.

The bugfix was also backported into f42 (util-linux-2.40.4-8.fc42).

The bug is in very old code (from 1997), so all older versions are affected.

John 2026-01-14 16:16:29 UTC

[Comment 3](#)

Status request: What is the timeline for backporting [CVE-2025-14104](#) to CentOS Stream 9?

Timeline data:

- CVE disclosed: Dec 2024 (13 months ago)
- Upstream fix: Available Dec 2024
- Fedora 43: Patched Dec 2024
- SUSE: Patched Jan 2026
- CentOS Stream 9: util-linux-2.37.4-21 (last update ~Feb 2025)

This affects SUID utilities in multi-user environments. A 13-month delay for a moderate CVE with available upstream fixes seems unusual for a security-focused distribution.

Is there a backport timeline or reason for the delay?

errata-xmlrpc 2026-02-02 10:05:16 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via RHSA-2026:1696 <https://access.redhat.com/errata/RHSA-2026:1696>

Matt 2026-02-03 14:50:13 UTC

[Comment 5](#)

Is there no intention to fix the [CVE-2025-14104](#) vulnerability for CentOS Stream 9?

Karel Zak 2026-02-04 07:25:27 UTC

[Comment 6](#)

The bugfix is expected in RHEL-9.8 and 10.2, it's already in the c10s branch

<https://gitlab.com/redhat/centos-stream/rpms/util-linux/-/commit/bde27314c01431821a0dd620a51643ab2170c40b>

and in c9s branch by commit:

<https://gitlab.com/redhat/centos-stream/rpms/util-linux/-/commit/22261c4fc3ece3f3d74ef4ea37aacc87c38eaf3d>

Karel Zak 2026-02-04 07:33:46 UTC

[Comment 7](#)

Adn builds:

<https://kojihub.stream.centos.org/koji/packageinfo?packageID=2257>

util-linux-2.37.4-24.el9	2025-12-15 11:02:17
util-linux-2.40.2-17.el10	2025-12-15 10:55:39

errata-xmlrpc 2026-02-04 11:05:01 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:1852 <https://access.redhat.com/errata/RHSA-2026:1852>

errata-xmlrpc 2026-02-04 19:48:41 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:1913 <https://access.redhat.com/errata/RHSA-2026:1913>

Note

You need to [log in](#) before you can comment on or make changes to this bug.