Util-linux: util-linux: heap buffer overread in setpwnam() when processing 256-byte usernames

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14104
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-05 17:16:03 UTC
Updated	2026-04-19 20:16:20 UTC
Description	A flaw was found in util-linux. This vulnerability allows a heap buffer overread when processing 256-byte usernames, specif

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from secalert@redhat.com

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

EPSS: 0.000070000 probability, percentile 0.004510000 (date 2026-04-19)

Problem Types: CWE-125 | CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Util-linux	Util-linux	affected 2.41.3 semver
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.40.2-15.el10_1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.32.1-48.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.32.1-48.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.37.4-21.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.37.4-21.el9_7 * rpm
CNA	Red Hat	Red Hat Ceph Storage 7	unaffected sha256:485411749726179fe5cd880e2cf308261b35150e4b356dd
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:2325f237ab329cb3f1d3db4da40ed19f68d6daa2a5902c71
CNA	Red Hat	Red Hat Ceph Storage 9	unaffected sha256:53a72419a7e4f4b332b9c6759ff1c389f226e26599236bc7
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.42-7.1.hum1 * rpm
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:975a1e501a8520df83f3f4114e72a71384ff1866ec99c7a45
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:48cf7cf48dfadb17f9357bf1894a5d0393551a893faa8b0ea
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:200c27e9b396276bd505c6b41127ac5eb1d94d620172cb8
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:d98fd3fe5f5f9acd0efae7db19b61b864be1eb2fbe2586a1b
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:5f1fbf66fb349a7baf066a1216d39989c3b89f18ec5108b96
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2025-14104	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3406	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:7180	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:1913	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2485	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:1696	secalert@redhat.com	access.redhat.com	

access.redhat.com/errata/RHSA-2026:4943	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2737	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2800	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2563	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:1852	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-12-05T14:16:36.004Z	Reported to Red Hat.
CNA	2025-12-05T00:00:00.000Z	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.