CVE-2026-3184

VEX

Public on February 25, 2026

Last modified: May 1, 2026 at 7:33:12 PM UTC

LOW

Low severity

What does this mean?

3.7

CVSS v3 Score Breakdown

Jump to section

Description Statement Mitigation Additional information Affected Packages CVSS Score Details Weakness (CWE) FAQ

Description

A flaw was found in util-linux. Improper hostname canonicalization in the `login(1)` utility, when invoked with the `-h` option, can modify the supplied remote hostname before setting `PAM_RHOST`. A remote attacker could exploit this by providing a specially crafted hostname, potentially bypassing host-based Pluggable Authentication Modules (PAM) access control rules that rely on fully qualified domain names. This could lead to unauthorized access.

Statement

This issue was rated as a Low severity issue. This is an authorization policy bypass limited to host-based access control decisions. It does not bypass authentication or grant elevated privileges. Exploitation is configuration-dependent and primarily affects legacy or uncommon remote login pathways, but it can violate administrator intent and weaken PAM-based security policy enforcement.

Mitigation

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.

Additional information

- Bugzilla 2442570: util-linux: util-linux: Access control bypass due to improper hostname canonicalization
- CWE-289: Authentication Bypass by Alternate Name

External references

- https://www.cve.org/CVERecord?id=CVE-2026-3184
- https://nvd.nist.gov/vuln/detail/CVE-2026-3184

Affected Packages and Issued Red Hat Security Errata

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.

Search:

Filter by: Products / Services | Components | State

Errata Clear all

Products / Services	Red Hat Hardened Images
Components	util-linux-main
State	Fixed
Justification	None
Errata	RHSA-2026:7180
Release Date	April 9, 2026

Products / Services	Red Hat Enterprise Linux 10
Components	util-linux
State	Not affected
Justification	Vulnerable Code not Present
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 7
Components	util-linux
State	Not affected
Justification	Vulnerable Code not Present
Errata	

1 of 1

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	CVE List
CVSS v3 Base Score	3.7	5.3	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	Low	N/A
Privileges Required	None	None	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	Low	Low	N/A
Availability Impact	None	None	N/A

CVSS v3 Vector

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

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

Understanding the Weakness (CWE)

CWE-289

Access Control

Technical Impact: Bypass Protection Mechanism

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?

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: May 1, 2026 at 7:33:12 PM UTC

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie preferences