



Bug 2442570 (CVE-2026-3184) - CVE-2026-3184 util-linux: util-linux: Access control bypass due to improper hostname canonicalization

Keywords: Security

Reported: 2026-02-25 07:56 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-25 08:19 UTC ([History](#))

Alias: CVE-2026-3184

CC List: 11 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-25 07:56:42 UTC

[Description](#)

Summary:

Improper hostname canonicalization in util-linux login(1) when invoked with -h can modify the supplied remote hostname before setting PAM_RHOST, potentially allowing bypass of host-based PAM access control rules (e.g., pam_access) that rely on fully qualified domain names.

Requirements to exploit:

An attacker must be able to access a remote login pathway that invokes login(1) with the -h <remotehost> option (e.g., telnet/rlogin-style daemons or custom wrappers). The target system must use PAM modules relying on PAM_RHOST for authorization decisions (such as pam_access) and have rules that distinguish between FQDNs and short hostnames. The local

system hostname must share the same domain suffix as the attacker-supplied hostname.

Note

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

