Bug 2324291 (CVE-2024-10963) - CVE-2024-10963 pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass

Keywords: Security ×

Status: NEW

Alias: CVE-2024-10963

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2324299 2324300

Blocks:

TreeView+ depends on / blocked

Reported: 2024-11-07 07:42 UTC by OSIDB Bzimport

Modified: 2024-11-09 13:46 UTC (History)

CC List: 0 users

Fixed In Version:

Doc Type: ---

Doc Text: A problem was found in pam_access where certain rules in its configuration file are mistakenly treated as hostnames. This means attackers could trick the system by pretending to be a trusted hostname, gaining unauthorized access. It's a risk for systems that rely on this feature to control who can access specific services or terminals.

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2024-11-07 07:42:58 UTC Description

A vulnerability in pam_access allows unauthorized users to bypass access restrictions by spoofing hostnames. This occurs because pam_access improperly interprets local access.conf rules to match remote hostnames, compromising configurations intended to restrict local access only. The issue affects all deployments using this configuration method, posing a significant risk to secure environments.

Note

You need to log in before you can comment on or make changes to this bug.