DECEPTION CHECK

Should this SSH account accept a password?

One host. One account. One evidence trail. SSHOLE / CVE-2026-123158.

01 / Check exposure **02 / Compare policy** **03 / Follow activity**

1. Name the service and owner

Host / stable identity / account

Owner / contact / review time (UTC)

Distribution / package / running service

Reachable SSH / PAM / password method

2. Fix the affected route

[ ] Applicability checked against the distribution advisory.

[ ] Fixed or backported package verified; running sshd restarted.

[ ] If temporarily disabling passwords, key access tested and a fresh login verified.

Record an applicability result, not shadow contents or password hashes. Root is not automatically reachable.

Change / verification evidence

3. Compare the accepted login with policy at that time

Event time / source / evidence reference

Account intended to use: [ ] keys only [ ] passwords allowed [ ] unknown

Policy source / valid interval / authorized change

Exactly one matching host/account state? [ ] yes [ ] no

Missing or overlapping policy is an unknown result, not a clean result. An accepted password that conflicts with policy is an investigation lead, not proof of this CVE.

4. Follow what happened next

[ ] Privilege use [ ] New accounts or SSH keys [ ] Processes [ ] Files [ ] Outbound traffic

For a requested download: distinguish command input, actual bytes received, and process execution.

Evidence / unresolved question

5. Assign the next action

[ ] Explained / authorized [ ] Policy anomaly [ ] Suspected compromise [ ] Collection gap

Action / owner / due time