CHECKLIST · SCAMS & SECURITY

A long password lets attackers into some Alpine Linux servers

Published 6 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/openssh-alpine-linux-password-bypass/

- [ ] **Ask who runs your Linux servers.** Ask your IT provider or host whether any of your servers, cloud machines or containers run Alpine Linux with SSH switched on.
- [ ] **Upgrade OpenSSH on every Alpine machine.** Run apk upgrade -U -a, then restart SSH with rc-service sshd restart. The upgrade alone leaves the old version running.
- [ ] **Switch off password logins.** Once key logins work, set PasswordAuthentication no, restart SSH with rc-service sshd restart, then check with sshd -T | grep -i passwordauthentication.
- [ ] **Patch every Alpine cloud machine from 3.18.11 to 3.24.3.** Those images ship a passwordless alpine user with admin rights. Update OpenSSH or switch off password logins on each running one.
- [ ] **Search the logs.** Look in /var/log/messages for "Accepted password for" root, alpine or any other account that has no password.
- [ ] **Treat any machine with a suspicious login as compromised.** If the logs can't rule out a login, don't keep trusting that machine.
- [ ] **Ask your router or device supplier.** Ask whether its firmware runs OpenSSH on musl, as OpenWrt and Buildroot builds can, and install any update.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.