*sshole: a passwordless SSH login on some Linux systems, and what to check

10 November 2026 · 5 min read · blogs.iictp.org/sshole-openssh-musl-linux-vulnerability

Security researchers reported this week that a flaw nicknamed *sshole lets an attacker log in to privileged accounts on some Linux systems without a password. Ars Technica reports that attackers are already using it.

TL;DR The short version

- A flaw nicknamed *sshole lets attackers log in to privileged accounts on some Linux systems without a password, and Ars Technica reports it is already being exploited.
- It comes from how OpenSSH interacts with musl, the lightweight C library used by Alpine Linux.
- Find hosts and container images that use musl and run OpenSSH, check the effective PAM configuration, and remember small base images change which code paths run.

Read online, listen to it, or change the text size: https://blogs.iictp.org/sshole-openssh-musl-linux-vulnerability

What was reported

According to Ars Technica, the flaw comes from how OpenSSH interacts with musl, a lightweight alternative to the standard C library that Alpine Linux uses. The report says a system is exposed when OpenSSH runs on musl **without** PAM (pluggable authentication modules), plus a few further conditions. Alpine configurations are affected, and other distributions may be if they match the same setup.

Ars also reports that the security firm GreyNoise saw attacks against its honeypots from a group it tracks as GT10, days after the flaw became public.

What a practitioner should do

- Find out which of your hosts and container images use musl (Alpine is the common one) and run OpenSSH. Images count, not only servers.
- Check whether those hosts run OpenSSH with PAM. Do not assume; read the effective configuration.
- Apply the vendor or distribution fix as soon as it is available, and watch your distribution’s security advisory for it.
- Until patched, reduce reach: restrict SSH to a management network or bastion, and turn off SSH where it is not needed.
- Review authentication logs for unexpected successful logins to privileged accounts.

The wider lesson

This is an Infrastructure & Security story with an architecture lesson inside it: small base images are chosen for good reasons, but they change which code paths run underneath your tools. Know what your base layer is, keep an inventory of it, and treat “nobody uses that configuration” as a claim to test, not a comfort. This is the kind of reasoning the TPBOK asks of a practitioner.

> Facts in this post were read from the sources listed below on 10 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. Ars Technica. Meet *sshole, the vulnerability that lets hackers SSH into Linux devices. 5 November 2026. arstechnica.com/security/2026/11/vulnerability-allows-attackers-to-log-into-some-linux-devices-sans-password/
2. Ars Technica. Vulnerability that lets hackers SSH into Linux devices is under active exploitation. 9 November 2026. arstechnica.com/security/2026/11/vulnerability-that-lets-hackers-ssh-into-linux-devices-is-under-active-exploitation/

Published by IICTP, an independent technical credential body, on 10 November 2026. The current version of this post is at https://blogs.iictp.org/sshole-openssh-musl-linux-vulnerability. More guides: blogs.iictp.org.