Meet *sshole, the vulnerability that lets hackers SSH into Linux devices

Devices running some configurations of Alpine Linux, and possibly other distributions, are affected by a decade-old vulnerability that allows attackers to log into devices with no password.

The vulnerability exists in the interaction between OpenSSH, the code library implementing SSH connections, and musl, a lightweight alternative to the libc library that, unlike most other Linux distributions, is used in Alpine. Further, OpenSSH using musl (pronounced muscle) must not use PAM (pluggable authentication modules), a framework that handles user authentication and account-access checks. Alpine is a lightweight, widely used Linux distribution. Other platforms may be affected if they use the same configurations.

One connection, works every time, needs no retries

There are two other conditions necessary for successful exploitation. First, a system must have at least one user account that’s accessible using a password that is hashed using the SHA256 or SHA512 functions. Second, the target system account must be configured to be passwordless, by way of specifying a “*” in the password field in /etc/shadow, the Linux file where password hashes are stored. Passwordless accounts are commonly used for accounts that use certificate-based authentication. This setting is common for certain types of accounts.

Read full article

Comments

https://arstechnica.com/security/2026/11/vulnerability-allows-attackers-to-log-into-some-linux-devices-sans-password/