SSH Hijacking Mitigation, Mitigation T1184 - Enterprise

Archived: 2026-04-05 17:52:08 UTC

Ensure SSH key pairs have strong passwords and refrain from using key-store technologies such as ssh-agent unless they are properly protected. Ensure that all private keys are stored securely in locations where only the legitimate owner has access to with strong passwords and are rotated frequently. Ensure proper file permissions are set and harden system to prevent root privilege escalation opportunities. Do not allow remote access via SSH as root or other privileged accounts. Ensure that agent forwarding is disabled on systems that do not explicitly require this feature to prevent misuse.

Source: https://attack.mitre.org/mitigations/T1184