Tailscale 1.104.4 Fixes SSH Flaws That Could Expose Root-Only Services on Other Servers



Tailscale released version 1.104.4 to fix flaws in its built-in SSH server that could let an attacker reach services and files on other servers meant only for root. Teams using Tailscale SSH should plan to update.

- Tailscale released version 1.104.4 to address flaws in its built-in SSH server.
- The flaws could let an attacker reach services and files on other servers that only root should access.
- They relate to how Tailscale SSH forwards network connections.
- The Tailscale background process performs that forwarding with root privileges.
- The source excerpt is truncated, so the attacker's preconditions are not confirmed here.

Tailscale has released version 1.104.4 to fix flaws in its built-in SSH server. According to the report, the flaws could allow an attacker to reach services and files on other servers that only the root user should be able to touch.

What is affected

The issues lie in how Tailscale SSH forwards network connections. This work is done by the Tailscale background process, which runs with root privileges. That is why a weakness in this path matters: the forwarding happens with far more authority than an ordinary user holds.

The source text available to us is cut off at the point where it describes what an attacker must do to exploit the flaws. We therefore cannot state the exact preconditions, and no CVE identifiers or severity scores appear in the excerpt. Readers should consult the vendor's release notes for those details.

What to do next

Organisations that use Tailscale SSH should identify where it is deployed and move those nodes to version 1.104.4. Where the feature is used to reach sensitive servers, it is worth reviewing which devices can connect to which hosts, since the reported risk concerns a compromised device reaching other servers.

This is a routine patching task rather than an emergency, but it should be handled through normal change management and tracked to completion.

What to do now

1. Inventory all hosts and devices running Tailscale SSH.
2. Upgrade affected Tailscale installations to version 1.104.4 through your change process.
3. Review the vendor's release notes for exploit preconditions and any further guidance.
4. Review access rules governing which devices may connect to which servers over Tailscale SSH.
5. Confirm after patching that nodes report the updated version.