

Public exploit released for AnyDesk Linux pre-authentication flaw giving root access



Researchers have published a working exploit for a pre-authentication remote code execution flaw in AnyDesk for Linux that grants root access. AnyDesk fixed it in version 8.0.3 in June, but described the fix only as a crash bug.

- A full working exploit for the AnyDesk Linux flaw is now public.
- The flaw allows remote code execution with root access before anyone approves a connection.
- The fix shipped in AnyDesk 8.0.3 in June.
- The changelog called it a bug that could lead to a crash; no CVE was assigned.
- Teams relying on changelog wording or CVE feeds may have missed the fix.

Security researchers have published a complete, working exploit for a flaw in AnyDesk for Linux. The vulnerability is a pre-authentication remote code execution issue, meaning an attacker does not need valid credentials, and it yields root access before any user approves the incoming connection.

What is known

AnyDesk addressed the flaw in version 8.0.3 in June. However, the changelog described the change only as a fix for a bug that could lead to a crash. No CVE was assigned and, according to the source, no security advisory accompanied the release. The source does not say whether the flaw has been exploited in the wild.

Why it matters

Because the fix was not labelled as a security update, organisations that prioritise patching based on CVE feeds or advisory wording may not have treated 8.0.3 as urgent. With a public exploit now available, any Linux system still running an earlier AnyDesk version should be considered exposed to a root-level compromise.

Recommended approach

The priority is to find every Linux host with AnyDesk installed, confirm its version, and update or remove it. Where remote access tools are not essential on servers, removal is the lower-risk option. Treat unexplained AnyDesk sessions or unexpected processes on affected hosts as items for investigation.

What to do now

1. Inventory all Linux hosts with AnyDesk installed and record their versions.
2. Update AnyDesk to 8.0.3 or later, or remove it where it is not required.
3. Restrict inbound AnyDesk connectivity to Linux servers and critical systems until patched.
4. Review logs on affected hosts for unexpected AnyDesk sessions or new root-level processes.
5. Add vendor release notes, not only CVE feeds, to the patch-intake process for remote access tools.