Barracuda discloses two flaws that can be chained to gain root access



Barracuda has disclosed two vulnerabilities that, if chained, let an attacker bypass authorization and reach root on a susceptible device. One is tracked as CVE-2026-116606 (CVSS 9.3).

- Two vulnerabilities affect Barracuda products: a pre-authentication authorization bypass and a command injection flaw.
- Chained together, they could give an attacker root access to a susceptible device.
- One flaw is identified as CVE-2026-116606 with a CVSS score of 9.3.
- The source excerpt does not name the affected products, versions or patches.

Barracuda has published details of two vulnerabilities in its products that can be combined to take full control of an affected device.

What was disclosed

The first flaw is a pre-authentication authorization bypass, meaning an attacker does not need valid credentials to exploit it. The second is a command injection vulnerability. Used in sequence, the two could let an attacker get past access controls and obtain root access on a susceptible device. One of the issues has been assigned CVE-2026-116606 and a CVSS score of 9.3, which places it in the critical range.

What is not yet clear

The material available to us does not list the affected products or versions, the identifier of the second flaw, or whether fixes and exploitation in the wild have been reported. Readers should not assume scope from the headline alone and should confirm these points directly with the vendor advisory.

Why it matters

Root access on a security or network appliance can expose the traffic, credentials and configuration the device handles. Because the first step needs no authentication, devices reachable from untrusted networks deserve attention first. A measured, inventory-led response is more useful than an emergency reaction before the facts are confirmed.

What to do now

1. Identify all Barracuda devices in your estate and record their models, versions and network exposure.
2. Review the official Barracuda advisory to confirm which products and versions are affected and whether patches are available.
3. Apply vendor fixes under your emergency change process once available, prioritising internet-facing or management-exposed devices.
4. Restrict administrative interfaces to trusted management networks until patching is complete.
5. Review logs on affected devices for unexpected authentication events or unusual commands, and escalate findings through your incident process.