HPE patches eight maximum-severity ArubaOS flaws allowing authentication bypass and RCE



HPE fixed 72 ArubaOS vulnerabilities, eight of them maximum severity, affecting AOS-8 and AOS-10. HPE reports no known exploitation or public exploit code yet, and urges prompt patching and restricted management access.

- HPE patched 72 vulnerabilities in ArubaOS, including eight rated maximum severity.
- The eight flaws affect multiple AOS-8 and AOS-10 versions and can be exploited remotely, without privileges or user interaction.
- They cover authentication bypass, command injection, SQL injection and buffer overflows, several leading to remote code execution (CVE-2026-79844 to CVE-2026-79851).
- HPE says it knows of no public exploit code or in-the-wild exploitation as of the advisory.
- HPE recommends restricting CLI and web management interfaces to a dedicated layer 2

> segment/VLAN or firewall-controlled access.

HPE has released security updates for 72 vulnerabilities in the Aruba Operating System (ArubaOS, also called AOS), which runs Aruba Networking enterprise wireless infrastructure such as mobility conductors, access points, controllers and gateways. Eight of the flaws carry the maximum severity rating.

What is affected

The eight flaws affect multiple AOS-8 and AOS-10 versions. A remote attacker with no privileges could exploit them through low-complexity attacks that need no user interaction. The issues include authentication bypass (including one in the PAPI protocol of AOS-10), unauthenticated command injection and SQL injection in AOS-8, and unauthenticated buffer overflows in AOS-10. Several of them lead to remote code execution. They are tracked as CVE-2026-79844 through CVE-2026-79851.

Exploitation status and vendor guidance

HPE states that it is not aware of public discussion or exploit code targeting these vulnerabilities, and has no evidence of exploitation in the wild as of the advisory date. It nevertheless urges customers to patch strongly, citing the complexity, breadth and impact of the flaws.

As a mitigation, HPE recommends restricting the command-line and web-based management interfaces to a dedicated layer 2 segment or VLAN, and/or controlling them with firewall policies at layer 3 and above, together with accounting controls that track and log user activity and resource usage.

Why it matters

Wireless controllers and gateways sit close to the core of the network. Institutions running AOS-8 or AOS-10 should treat this as a priority change, even though no exploitation has been reported, because the absence of public exploit code tends to be temporary.

What to do now

1. Inventory all Aruba devices running AOS-8 or AOS-10 and identify affected versions against the HPE advisory.
2. Schedule and apply the HPE patches as an expedited change, starting with internet-reachable or poorly segmented controllers.
3. Restrict CLI and web management interfaces to a dedicated layer 2 segment/VLAN and/or firewall rules at layer 3 and above.
4. Enable accounting and logging of administrative activity and review logs for unexpected access to management interfaces.
5. Record the exposure and remediation in your vulnerability management process, and monitor for any

later reports of exploitation.