NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-61514

Summary

CVE-2026-61514 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. Puwell IP Camera firmware versions 2.x through 4.x contains an authentication bypass vulnerability that allows unauthenticated attackers to access device functions by sending protocol-conforming packets over TCP port 23456 without credentials. Attackers can exploit the unvalidated Session field in the proprietary control protocol header to access live video streams, control pan and tilt motors, activate audio functions, and remotely restart the device.

What we know

- **CVE:** CVE-2026-61514
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.