EXPLOITED VULNERABILITY ADVISORY: CVE-2026-72530

Summary

CVE-2026-72530 in TrueConf Server is being actively exploited in the wild. A remote unauthorized attacker with network access via port 4307/TCP to the TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier could use a specially crafted script to break out of the isolated environment and execute arbitrary code on the host system. CISA requires federal remediation by 2026-09-03; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-72530
- **Affected:** TrueConf Server
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-20
- **Severity:** CVSS 9.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 1%
- **Weakness:** CWE-94

Recommended action

Patch CVE-2026-72530 by 2026-09-03. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.