EXPLOITED VULNERABILITY ADVISORY: CVE-2026-8037

Summary

CVE-2026-8037 in Progress LoadMaster is being actively exploited in the wild. OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an un-authenticated attacker to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in multiple command endpoints CISA requires federal remediation by 2026-08-10; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-8037
- **Affected:** Progress LoadMaster
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-07
- **Severity:** CVSS 9.6 Critical, Adjacent_Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 85%
- **Weakness:** CWE-77

Recommended action

Patch CVE-2026-8037 by 2026-08-10. If you cannot patch immediately, apply available vendor mitigations and monitor for exploitation until patched. 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.