

CVE-2026-8037

Progress LoadMaster Command Injection Vulnerability

CISA KEV since Aug 7, 2026

Actively exploited

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

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.774 99.56th percentile · FIRST	CISA DEADLINE Aug 10, 2026 CISA federal deadline · Overdue by 2 months
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.774 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connection manager for objectscale	< 7.2.63.2	7.2.63.2	NVD
ecs connection manager	< 7.2.63.2	7.2.63.2	NVD
moveit web application firewall	< 7.2.63.2	7.2.63.2	NVD
loadmaster	< 7.2.54.18 ≥ 7.2.55.0 < 7.2.63.2	7.2.54.18 · 7.2.63.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-57pc-jm9r-hgjj4	Additional guidance	community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-8037	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-34260	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-8037

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.