An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606160511

NCSC Advisory

Progress Software: ECS Connections Manager, LoadMaster, Object Scale Connection Manager, MOVEit WAF Critical Vulnerability.

CVE-2026-8037

17th, June 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-8037

Published: 2026-06-04

Vendor: Progress Software

Product: ECS Connections Manager, LoadMaster, Object Scale Connection Manager, MOVEit WAF

CVSS Score[1]: 9.6

Products Affected

Product	Version
LoadMaster	V7.2.60.0 < V7.2.63.2
LoadMaster	V7.2.45.12 < V7.2.54.18
ECS Connections Manager	V7.2.60.0 < V7.2.63.2
Object Scale Connection Manager	V7.2.60.0 < V7.2.63.2
MOVEit WAF	V7.2.60.0 < V7.2.63.2

Impact

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. An unauthenticated remote attacker exploits unsanitized input in the LoadMaster API command endpoints to inject arbitrary OS commands, resulting in full remote code execution on the appliance.

Common Weakness Enumeration (CWE)[2]: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

---

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Progress Software.

- https://nvd.nist.gov/vuln/detail/CVE-2026-8037
- https://www.cve.org/CVERecord?id=CVE-2026-8037
- https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691