INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-30 14:48 UTC

CVE-2026-8037: Unauthenticated Root RCE in Progress Kemp LoadMaster Reaches Public PoC Stage

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0373
Type	CVE Vulnerability
CVE ID	CVE-2026-8037, CVE-2026-33691, CVE-2024-1212
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0187 (77th percentile)
Affected Products	Progress Kemp LoadMaster, GA v7.2.63.1 and older, LTSF v7.2.54.17 and older
Published	2026-06-30T03:38:07
Discovery Source	Rss

Executive Summary

A CVSS 9.5 unauthenticated remote code execution vulnerability in Progress Kemp LoadMaster, tracked as CVE-2026-8037, allows an attacker with network access to the management interface to execute arbitrary commands as root without any credentials. A public proof-of-concept was published by watchTowr Labs on June 29, 2026, materially narrowing the window before exploitation attempts are likely. Organizations running LoadMaster GA v7.2.63.1 or older, or LTSF v7.2.54.17 or older, should treat patching as an emergency action. A co-disclosed vulnerability, CVE-2026-33691, is also addressed in the same patch. The predecessor vulnerability on this same product, CVE-2024-1212 (CVSS 10.0), experienced confirmed in-the-wild exploitation and CISA KEV listing.

Technical Analysis

CVE-2026-8037 (CVSS 9.5) is an OS command injection vulnerability in Progress Kemp LoadMaster's /accessv2 API endpoint. A missing null terminator in the input sanitization function allows an unauthenticated remote attacker to inject and execute arbitrary OS commands as root. CWE mappings: CWE-78 (OS Command Injection), CWE-131 (Incorrect Calculation of Buffer Size), CWE-170 (Improper Null Termination), CWE-134 (Use of Externally-Controlled Format String). Affected versions: GA v7.2.63.1 and older; LTSF v7.2.54.17 and older. A second CVE, CVE-2026-33691, is co-disclosed in the same Progress June 2026 security bulletin;

independent severity and full technical details for that CVE are not fully characterized from available source data. MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1059/T1059.004 (Command and Scripting Interpreter), T1068 (Exploitation for Privilege Escalation), T1133 (External Remote Services), and T1078.001 (Default Accounts). watchTowr Labs published a public PoC on June 29, 2026 (GitHub Advisory GHSA-57pc-jm9r-hgj4). Patches are available per the Progress security bulletin. No confirmed active exploitation of CVE-2026-8037 has been reported in the source data as of the time of writing; exploitation probability is assessed as elevated given PoC availability and the exploitation history of CVE-2024-1212 on the same platform.

Action Checklist

1. Step 1: Containment. Identify all LoadMaster instances running GA v7.2.63.1 or older, or LTSF v7.2.54.17 or older (per the Progress June 2026 Critical Security Bulletin). Restrict network access to the LoadMaster management interface (/accessv2 API endpoint) to trusted administrative IP ranges via firewall ACL or perimeter controls. If management access cannot be restricted, take the appliance offline until patching is complete. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Query web server and API access logs on LoadMaster for anomalous or unexpected requests to the /accessv2 endpoint, particularly from untrusted source IPs or with malformed input patterns consistent with command injection (semicolons, pipe characters, shell metacharacters in parameter values). Review system-level command execution logs and OS audit logs for unexpected root-level process spawning. Enable and review audit event logs per NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting). Monitor for indicators associated with T1190 and T1059 in SIEM. Apply D3-LAM (Local Account Monitoring) to detect unauthorized root-level activity post-exploitation.
3. Step 3: Eradication. Apply the patches specified in the Progress LoadMaster Critical Security Bulletin, June 2026 (CVE-2026-8037, CVE-2026-33691) available at the Progress community portal. Upgrade GA track to a version newer than v7.2.63.1 and LTSF track to a version newer than v7.2.54.17 per vendor upgrade guidance. Confirm CVE-2026-33691 is also remediated by the applied patch, given co-disclosure in the same bulletin. Reference: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, verify the installed LoadMaster version against the fixed version listed in the Progress bulletin. Conduct a post-patch review of LoadMaster access logs and OS audit logs for any evidence of prior exploitation (unexpected root commands, new accounts, dropped files, modified configurations). Re-enable management interface access only after confirming the patch is applied and no indicators of compromise are present. Monitor the /accessv2 endpoint and root-level process activity for a minimum of 30 days post-remediation. Apply D3-SFA (System File Analysis) to detect any configuration or binary tampering that may have preceded patching. Reference: NIST AU-11 (Audit Record Retention), AU-6.
5. Step 5: Post-Incident. Assess whether management interfaces for network infrastructure are adequately isolated from internet-facing networks and from general user segments; this vulnerability class (unauthenticated API exposure) is a recurring pattern on LoadMaster (see CVE-2024-1212 precedent). Review and update the vulnerability management process to ensure internet-facing load balancer firmware is included in automated patch tracking cycles. Consider whether a WAF or API gateway with input validation sits in front of LoadMaster management APIs. Document control gaps against NIST AC-4

(Information Flow Enforcement) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process). Apply D3-CH (Credential Hardening) and D3-UAP (User Account Permissions) to reduce blast radius if a similar vulnerability is exploited in the future.

Detection Guidance

Focus detection on the /accessv2 API endpoint on all LoadMaster instances. Query access logs for requests to /accessv2 from sources outside defined administrative IP ranges. Look for parameter values containing OS command injection metacharacters: semicolons (;), pipe characters (|), backticks (`), dollar-sign subshells ($(...)), and newline sequences. In OS-level audit logs, look for root-level process spawning triggered by the LoadMaster application process, particularly shell processes (sh, bash, ash) forked from the web server or API handler process. Cross-reference with MITRE T1190 (Exploit Public-Facing Application) and T1059.004 (Unix Shell). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence: review daily until patched, not weekly. Use D3-LAM (Local Account Monitoring) to flag new local accounts or privilege changes on LoadMaster appliances. EPSS score is 0.01869 (76.71st percentile) at time of reporting; this will likely increase following PoC publication, re-check EPSS regularly. No specific IOC hashes, IPs, or domains are available from the provided source data at this time.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1078.001** — Default Accounts
- **T1059** — Command and Scripting Interpreter
- **T1068** — Exploitation for Privilege Escalation
- **T1059.004** — Unix Shell
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing

- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1078.001	Default Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059.004	Unix Shell	Execution
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/progress-kemp-loadmaster-flaw-cou...	T2

Source	URL	Tier
LoadMaster Critical Security Bulletin – June 2026 – (CVE-2026 ...	https://community.progress.com/s/article/LoadMaster-Critical-Securi...	T3
CVE-2026-8037 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
OS Command Injection Remote Code Execution Vulnerability...	https://github.com/advisories/GHSA-57pc-jm9r-hgj4	T1
CVE-2026-33691 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33691	T1

Generated 2026-06-30 14:48 UTC by TJS Security Command Center