Observed Exploitation Attempts Targeting Critical Progress Kemp LoadMaster Vulnerability (CVE-2026-8037)

Jul 01, 2026

WHITE

View Alert

On June 29, 2026, eSentire's Threat Response Unit (TRU) identified active, in-the-wild exploitation attempts targeting a critical flaw in Progress Kemp LoadMaster appliances, tracked as CVE-2026-8037. This tracking follows the public release of a functional Proof-of-Concept (PoC) exploit code on the same day, which significantly elevated the immediate threat landscape for exposed environments.

Organizations using affected versions of the load balancer are urgently advised to verify their device configurations and apply the firmware patches to prevent unauthorized network entry.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to this vulnerability.

Additional Info

Analysis:

Progress Kemp LoadMaster is an Application Delivery Controller (ADC) and load balancer widely positioned at the perimeter of corporate networks to manage Layer 4 and Layer 7

traffic, perform SSL/TLS offloading, and provide Web Application Firewall (WAF) services. Because these edge appliances bridge the open internet and internal corporate assets, they are highly attractive targets for threat actors. The critical vulnerability affecting the application carries a severe CVSS score of 9.8 and allows unauthenticated attackers to execute arbitrary code with systemic privileges.

The security defect stems from improper input validation and memory handling within the management API's ***escape_quotes()*** function, which is exposed to the internet via the ***/accessv2*** API endpoint. Technical analysis by watchTowr Labs revealed that when handling user-supplied string data, the application uses ***malloc()*** to allocate a heap buffer but fails to properly initialize or null-terminate the newly escaped string. This creates an out-of-bounds read condition, allowing data from adjacent, uninitialized heap memory to persist. By strategically manipulating heap allocation states, a remote attacker can trick the system into inserting payload commands directly into a shell command context that is subsequently processed by the underlying ***system()*** function.

Exploiting this uninitialized heap memory and command injection vulnerability enables a completely unauthenticated, remote attacker to achieve pre-authentication Remote Code Execution (RCE). An attacker does not need legitimate administrative credentials or prior authentication to trigger the exploit sequence. Once code execution is established, adversaries can run arbitrary terminal commands, compromise the appliance's integrity, steal sensitive data, and use the device's privileged network position to pivot deep into internal enterprise infrastructure.

Although the flaw was initially disclosed by Progress on June 4, 2026, the arrival of functional public exploit code on June 29 rapidly transitioned the flaw from a theoretical risk to a live threat vector. While eSentire’s Threat Response Unit noted that its monitored instances successfully contained or repelled the initial exploitation attempts without post-compromise activity, the threat intelligence unit assesses that mass exploitation attempts are highly probable to accelerate. This vulnerability impacts all configurations where the management API feature is enabled across specific product baselines, specifically affecting Progress Kemp LoadMaster General Availability (GA) Track version

7.2.63.1 and all prior versions, as well as Long-Term Support Feature (LTSF) Track version 7.2.54.17 and all prior versions.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Apply official vendor patches to move deployments out of vulnerable states.
- Download upgrades strictly through the official Progress Download Hub and validate the files using the corresponding XML checksums.
- Turn off the management API functionality if it is not operationally required.
    - If the API must remain active, use firewall rules or access control lists (ACLs) to ensure the /accessv2 endpoint is accessible only from trusted internal administrative IPs.
- Review the Guidance and Strategies to Protect Network Edge Devices resources.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	4d91f025
Category	Threat Bulletins
References	cisa progress thehackernews watchtowr hhs thehackernews 1 esentire
Tags	Progress Kemp LoadMaster, CVE-2026-8037

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--