Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical RCE Vulnerability Hits Progress LoadMaster

Date of Publication	Admiralty Code	TA Number
September 9, 2024	A1	TA2024346

Summary

First Seen: September 2024
Affected Products: LoadMaster, LoadMaster Multi-Tenant (MT) hypervisor
Impact: A critical vulnerability, identified as CVE-2024-7591, has been discovered in the LoadMaster product line, affecting all LoadMaster releases and the LoadMaster Multi-Tenant (MT) hypervisor. This flaw arises from improper input validation, enabling an unauthenticated remote attacker to access the LoadMaster management interface through a specially crafted HTTP request. Progress Software has issued an emergency fix for this vulnerability, which carries a maximum severity rating of 10/10.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-7591	Progress LoadMaster OS Command Injection Vulnerability	LoadMaster, LoadMaster Multi-Tenant (MT) hypervisor	✗	✗	✓

Vulnerability Details

#1 Progress Software has issued an emergency fix for a critical vulnerability identified as CVE-2024-7591, which affects its LoadMaster and LoadMaster Multi-Tenant (MT) Hypervisor products. This flaw, which has been assigned the maximum severity rating of 10/10, allows attackers to remotely execute commands on the device.

#2 Progress LoadMaster is a family of advanced load balancing appliances designed to optimize application performance, enhance security, and ensure high availability by distributing network traffic across multiple servers. These devices are commonly deployed in data centers and enterprise environments to manage traffic for web services, applications, and network resources.

#3 CVE-2024-7591 is particularly concerning because it allows unauthenticated remote attackers to exploit the vulnerability by sending a specially crafted HTTP request to the LoadMaster management interface. This could lead to the execution of arbitrary commands on the system, potentially resulting in full system compromise. The insufficient sanitization of user input exacerbates the risk.

#4 To mitigate the risk posed by CVE-2024-7591, Progress Software has released an add-on package that can be installed on all vulnerable versions of LoadMaster, including older releases. Importantly, this patch can be applied without needing to upgrade to a specific version. However, it's crucial to note that this patch does not cover the free version of LoadMaster, leaving those users still exposed to this critical vulnerability.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7591	LoadMaster 7.2.60.0 and all prior versions, Multi-Tenant Hypervisor 7.1.35.11 and all prior versions	cpe:2.3:a:progress:loadmaster:*:*:*:*:*:*:*	CWE-20

Recommendations

Update: To mitigate the risk posed by the critical vulnerability CVE-2024-7591, users are strongly encouraged to download and install the emergency add-on package immediately. Installation can be done through the System Configuration > System Administration > Update Software UI page.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	

Patch Details

To address the risk posed by CVE-2024-7591, customers should apply the add-on package released by Progress Software. This package can be installed on any version of LoadMaster, even if support for the unit has expired.

Patch Link:
https://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591

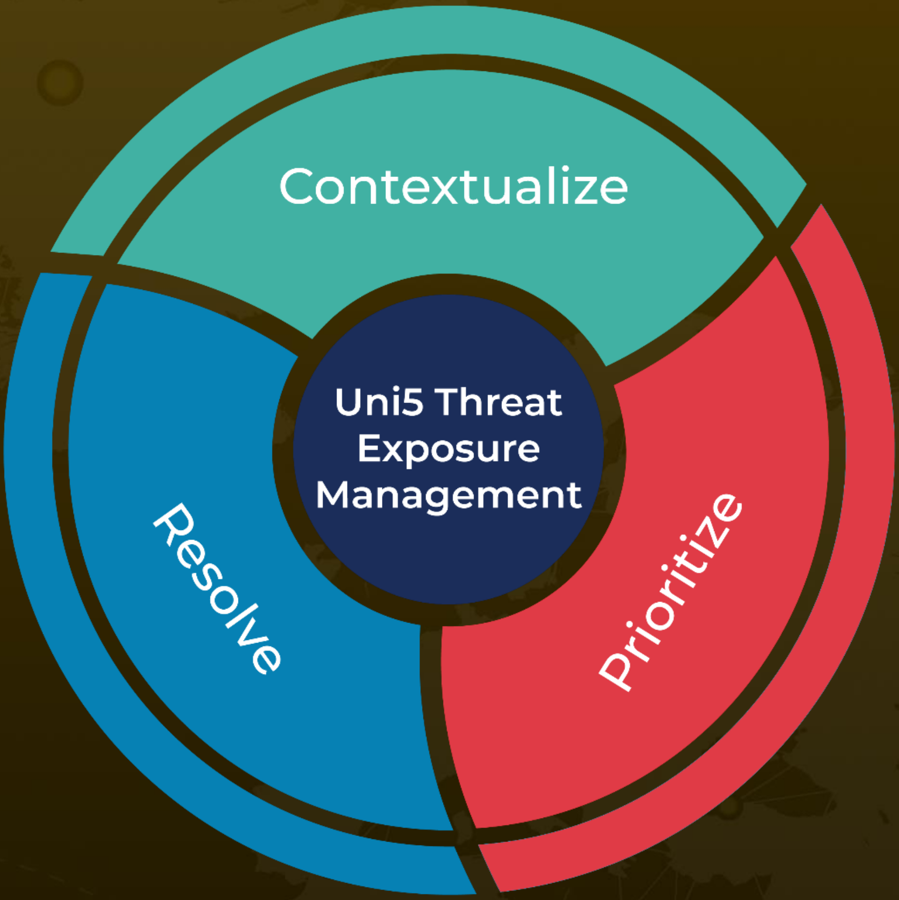
References

https://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 9, 2024 • 6:00 AM

More at www.hivepro.com