Progress®
Kemp® LoadMaster®

LoadMaster 7.2.54.13 Release Notes

Generated on: 11 March 2025

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Chapter 2: Before You Upgrade (READ ME FIRST) 5

Supported Models for Upgrade 6

Upgrade Path 7

Upgrade Patch XML File Verification Notes 7

Code Signing Certificate Update 8

Chapter 3: Security Updates 9

Chapter 4: New Known Issues 11

Chapter 5: Issues Resolved 12

Chapter 6: Existing Known Issues 14

1

Introduction

LoadMaster Operating System (LMOS) version 7.2.54.13 is a security and bug fix update of the Long Term Support Feature (LTSF) branch made available on 5 February 2025. Please read these release notes before upgrading to this version.

2

Before You Upgrade (READ ME FIRST)

Please pay special attention to the issues below before you begin an upgrade to this release.

Generation of 4096-bit DHE Key

During an upgrade to this version from a version prior to 7.2.53.0, a new 4096-bit DHE key is generated. On some virtual or hardware appliances, this can lead to significant CPU and memory consumption that could impact regular Virtual Service traffic. Progress Kemp strongly recommends that updates to this release from a version prior to 7.2.53.0 be performed during a maintenance interval.

Best Practices Cipher Set

In 7.2.52.0, the **BestPractices** cipher set was updated. If you are upgrading from a version prior to 7.2.52.0, this change is effective immediately after upgrading to this release. This change was made to improve security and conform to the latest industry best practices.

Note: If you depend on any of the cipher sets being removed from the BestPractices set, then *before you upgrade* you must create a custom cipher set that contains these ciphers and assign this new custom cipher set to the Virtual Services that are currently using the BestPractices cipher set. After this is done, you can upgrade to this release and your services will continue to use the old ciphers. If you do not, then after upgrading, any clients that depend on these ciphers being available will no longer be able to connect.

It is recommended, however, that you migrate your services as soon as possible to use the new **BestPractices** cipher set.

Contents

- Supported Models for Upgrade
- Upgrade Path
- Upgrade Patch XML File Verification Notes

Supported Models for Upgrade

This LoadMaster release is supported on the Hardware and Virtual models shown in the first two columns of the table below. *It is not supported and should not be installed on any model listed in the column at right.* This update patch can be applied to any supported model regardless of licensing (for example, Service Provider License Agreement (SPLA) or Metered Enterprise License Agreement (MELA)) or platform (for example, hardware, local cloud, or public cloud).

Note that as of February 1, 2025, the following models have reached their end of life (EOL) and are no longer supported:

- LMB-1G
- LMB-2G
- LMB-5G
- LMB-10G
- LM-8000
- LM-8010-MT
- LM-8020
- VLM-200
- VLM-5000
- VLM-10G

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Models
VLM-500	LM-X25-NG	LMB-MAX	VLM-200
VLM-2000	LM-X40-NG		VLM-5000
VLM-3000	LM-X40M-NG		VLM-10G
VLM-3000	LM-XHC-25G-NG		LM-8000
VLM-GEO	LM-XHC-40G-NG		LM-8010-MT
VLM-MAX	LM-XHC-100G-NG		LM-8020
VLM-SPLA-50	LM-X1		LMB-1G
VLM-SPLA-100	LM-X3		LMB-2G
VLM-SPLA-500	LM-X15		LMB-5G

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Models
VLM-SPLA-3000	LM-X25		LMB-10G
VLM-SPLA-GEO	LM-X40		LM-2000
	LM-X40M		LM-2200
	LM XHC 25G		LM-2400
	LM XHC 40G		LM-2500
	LM XHC 100G		LM-2600
	LM-3000		LM-3500
	LM-3400		LM-3600
	LM-4000		LM-5000
	LM-5600		LM-5300
	LM-8020M		LM-5500
	LM-X3-NG		LM-Exchange
	LM-X15-NG		LM-GEO
	LM-X25MT-NG		LM-UCS Series
	LM-XHC55-NG		LM-R320
	LM-XHC75-NG		LM-5400
			LM-8020-FIPS
			VLM-100
			VLM-1000

Upgrade Path

You can upgrade to this release from any previous 7.2.x release. For full upgrade path information, refer to one of the following documents:

- Updating the LoadMaster Software Technical Note (Long Term Support Feature (LTSF) version)
- Updating the LoadMaster Software Technical Note (General Availability (GA) version)

Upgrade Patch XML File Verification Notes

By default, verification of the digital signature on upgrade images is required in LMOS 7.2.50.0 and above.

See the **Update Verification Options** setting under **System Administration > Miscellaneous Options > WUI Settings**. If the unit you are upgrading is set to require validation, you must supply the XML Verification File supplied with this release.

Note that:

- In previous releases, *two* verification files were provided: one for pre-7.2.51 systems and one for later systems. This restriction has been removed with the 7.2.53.0 release; if upgrading from firmware 7.2.51.0 / 7.2.48.3 and above you can use the XML file provided with this release. If upgrading from any other firmware version you must following the upgrade path detailed in the Updating the LoadMaster Software Technical Note.
- Appliances running an LMOS version prior to 7.2.49 do not provide the option of XML file verification in the UI or API. If you are upgrading from one of these releases to this release, you can verify the digital signatures offline. For further information, refer to the Verifying XML Signatures Technical Note.

Contents

- Code Signing Certificate Update

Code Signing Certificate Update

On 27 May 2022, the certificate used to sign LoadMaster release artifacts for LoadMaster LMOS version 7.2.54.4 and prior releases expired. Starting with 7.2.54.5, all LTSF releases will be signed with a new certificate. For details on how this might affect you, refer to the following article: LoadMaster Code Signing Certificates and LTSF Releases.

All LTSF releases after that occur after the above date (LMOS 7.2.54.5 and later) will be digitally signed using a newly obtained code signing certificate.

3

Security Updates

Fixes For Multiple Vulnerabilities

Fixes for the following security vulnerabilities are included in this release.

Refer to the related Support Knowledge Base article for more information.

Fixes for CVE-2024-56131 / CVE-2024-56132 / CVE-2024-56133 / CVE-2024-56135

Remote malicious actors who gain access to the management interface of the LoadMaster and successfully authenticate could issue a carefully crafted HTTP request that allows arbitrary system commands to be executed. This vulnerability has been closed by sanitizing request user input to mitigate arbitrary system commands being executed.

Fix for CVE-2024-56134

Remote malicious actors who gain access to the management interface of the LoadMaster and successfully authenticate could issue a carefully crafted HTTP request that allows the content of any file on the system to be downloaded. This vulnerability has been closed by sanitizing request user input to mitigate arbitrary system commands being executed.

Fixes Previously Delivered in Add-On Packages

A fix for the following security vulnerability, previously delivered via an add-on package, is included in this release. If you have previously installed an add-on package to address this vulnerability, the add-on package whose name matches the CVE number below can now be removed during your next maintenance cycle. [Note that leaving the add-on installed will not cause any issues.]

- CVE-2024-8755

4

New Known Issues

LM-7112	**System Configuration > Network Setup > Interfaces UI**: When removing an interface from a bond, spurious text beginning with “Cannot find device…” may appear in the background, behind the confirmation pop-up. This text can be ignored.

5

Issues Resolved

LM-7034	**L7 Kernel**: A timing issue in the L7 kernel has been identified that could cause a crash and a system reboot. Essentially, a client connection closes unexpectedly and the corresponding destination socket is in an undefined state. This issue has been fixed.
LM-6721	**QoS**: Fixed an issue observed starting in 7.2.60.0 where logging for limited connections did not always occur as expected.
LM-6620 LM-6630	**System Console**: Fixed issues seen starting with 7.2.60.1 that caused spurious messages to appear on the system console on booting into non-FIPS and FIPS modes.
LM-6618	**ACME Application Programming Interface (API)**: Fixed an issue that caused the API command for registering a DigiCert account to fail.
LM-6591	**Web Application Firewall (WAF) API**: Fixed an issue where rapid custom rule uploads could remove previously applied rules.
LM-6589	**ACME**: The certificate repository appears as blank for a read only user. This issue has been fixed.
LM-6584	**ACME API**: Fixed an issue where an invalid JSON format response is returned when retrieving a certificate using *getacmecert*.
LM-6581	**ACME**: Fixed an issue with certificate deletion observed in High Availability (HA) mode.
LM-6520	**APIv2**: Fixed an issue where a plus sign (+) included in an APIv2 (JSON) format call is replaced with a space.
LM-6366	**GEO**: Fixed an issue observed in 7.2.59 where only a subset of the defined GEO custom locations is displayed under FQDN location based scheduling.

LM-6191	**Interface Settings**: Fixed an issue where MTU changes for bonded interfaces and VLANs did not take effect.
LM-6190	**GEO**: In previous releases, if the zone name is not set, a serverfail error is returned when querying the (Source of Authority) SOA record. This issue has been fixed.
LM-6184	**Single Sign On (SSO)**: Authentication using reCaptcha fails when the size of the token is above 800 bytes. The maximum number of bytes supported for a token has been increased to 4K.
LM-5923	**APIv2**: Corrected format errors in the JSON output of the "stats" command for QoS/Limited client IP addresses.
LM-5709	**QoS / Limiting**: Fixed an issue that caused spurious "Client x.x.x.x no longer limited" messages to appear in the system log.
LM-5698	**GEO**: Fixed an issue first seen in 7.2.59 where the "Disabled Clusters Unavailable" setting is turned on, but disabled clusters are still reported as available.
LM-5627	**GEO Debug Info**: Fixed an issue that caused the Config Version / SOA serial number to no longer match between GEO partners.
LM-5383	**GEO**: Fixed an issue where deleting a custom location on one partner does not take effect on the other partner.
LM-5182	**Single Sign On (SSO)**: Fixed an NTLM authentication issue that caused user access check control errors when the username is in UPN format and the domain specified is a domain other than the SSO domain.
LM-4957	**GEO Logging**: In previous releases, logs showing IP addresses as "administratively disabled" are printed to the log whenever any administrative change is made to GEO. This issue has been fixed.
LM-2744	**SAML Authentication**: Fixed an issue that could cause a logout loop.
LM-2739	**Idle Connection Timeout:** In previous releases, the default idle connection timeout setting was not working properly until it was explicitly re-set. This issue has been fixed.
LM-2404	**WAF**: Fixed issues that caused the WAF engine to become temporarily unresponsive when being scanned by tenable.io.
LM-1007	**GEO**: In previous releases, IP addresses shown in the IP Remote VS selection menu that apply to multiple ports have no ports listed. The display has been modified to include a list of all ports that apply to the IP address (for example, 10.10.10.10:[80, 90]).
LM-570	**GEO**: In previous releases, it was possible to delete an IP Address Range that is configured for use by an FQDN. With this release, you cannot delete an IP address range that is in use.
LM-126	**GEO**: Fixed an issue causing a spurious message to be displayed on the system console (disp_addrr_elements is not defined).

6

Existing Known Issues

LM-6580	**OpenSSH**: The version of OpenSSH used in FIPS mode is vulnerable to CVE-2024-6387 which will be addressed in a future release. To mitigate this issue, ensure that the system management interface is located on a restricted, secure network that can only be accessed by trusted personnel, as described in our security hardening guidelines.
LM-5339	**Single Sign On (SSO)**: When **Failed Login Attempts** is set to 0, a user logging in using invalid credentials (for example, the wrong password) will fail to log in, as expected; however, the login will also be blocked. The workaround is to set **Failed Login Attempts** to a higher value.
LM-5019	**GEO Clusters:** Under specific circumstances, there is a small timing window during which cluster checks may fail, resulting in the cluster being erroneously marked down.
LM-5303	**Certificate UI**: A certificate having a Common Name (CN) set to the wildcard character (*) displays unrelated text in the UI. This is a cosmetic issue that affects the UI only.
LM-4898	**PowerShell API**: PS cmdlets related to Let's Encrypt are not working.
LM-4121	**GEO**: If you add a Zone Name to GEO *after* you created working FQDNs, GEO may no longer respond to queries for one or more of the FQDNs after the Zone Name is added. The workaround is to remove and then re-add the FQDNs that are no longer working.
LM-3942	**LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI.
LM-3929	**Content Rule UI**: Display is incorrect when the 'Ignore case' option is enabled.
LM-3789	**Stability**: In rare cases, an unexpected reboot may occur as the system is stopping a Virtual Service (because, for example, there are no Real Servers available). If a new connection to the Virtual Service is

	received during a very short period of time during the process of stopping the Virtual Service, then the system may reboot.
LM-3095	**FIPS: OCSP: LDAPS**: The LoadMaster should not authenticate a user from LDAPS server if the chain is not complete
LM-3094	**UI / Templates**: An issue that causes format breakage in the UI when a non-certificate file is uploaded as an intermediate certificate
LM-2749	**API Keys**: An API key created for a remotely managed user (for example, RADIUS) will not work unless the remote user ID is also added as a local user on LoadMaster.
LM-1038	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
LM-143	**ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service.
LM-136	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.