

LoadMaster 7.2.54.10 Release Notes

Generated on: 18 December 2024

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

Chapter 3: Security Updates 8

Chapter 4: Issues Resolved. 9

Chapter 5: Existing Known Issues 10

1

Introduction

LMOS Version 7.2.54.10 is a security and bug fix update of the Long Term Support Feature (LTSF) branch made available on 30 April 2024. This update closes the security vulnerabilities described in CVE-2024-3544 and CVE-2024-3543; refer to the remaining sections of these notes for additional details. Please read the sections in this Release Notes document before installing or upgrading to this release.

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.

Related Links

For details, see the following topics:

- Supported Models for Upgrade
- Upgrade Path

Supported Models for Upgrade

This release of LMOS is supported on the Hardware and Virtual models shown in the first three 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).

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models
VLM-200	LM-X25-NG	LMB-1G	LM-2000
VLM-500	LM-X40-NG	LMB-2G	LM-2200
VLM-2000	LM-X40M-NG	LMB-5G	LM-2400
VLM-3000	LM-XHC-25G-NG	LMB-10G	LM-2500
VLM-5000	LM-XHC-40G-NG	LMB-MAX	LM-2600
VLM-10G	LM-XHC-100G-NG		LM-3500
VLM-GEO	LM-X1		LM-3600
VLM-MAX	LM-X3		LM-5000
VLM-SPLA-50	LM-X15		LM-5300
VLM-SPLA-100	LM-X25		LM-5500
VLM-SPLA-500	LM-X40		LM-Exchange
VLM-SPLA-3000	LM-X40M		LM-GEO
VLM-SPLA-GEO	LM XHC 25G		LM-UCS Series
	LM XHC 40G		LM-R320
	LM XHC 100G		LM-5400
	LM-3000		LM-8020-FIPS
	LM-3400		VLM-100

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models
	LM-4000		VLM-1000
	LM-5600		
	LM-8000		
	LM-8020		
	LM-8020M		

Upgrade Path

You can upgrade to this release from any previous 7.2.x release. For full upgrade path information, refer to the following article: Firmware Upgrade Path.

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 Firmware Upgrade Path article.
- 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.

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

Fix for CVE-2024-3544

Unauthenticated attackers can perform actions, using SSH private keys, by knowing the IP address and having access to the same network of one of the machines in the High Availability (HA) or Cluster group. This vulnerability has been closed by enhancing LoadMaster partner communications to require a shared secret that must be exchanged between the partners before communication can proceed. The new **Partner Communications** shared secret parameter is located on the **Certificates & Security > Remote Access** page of the User Interface (UI).

Fix for CVE-2024-3543

Use of a reversible password encryption algorithm allows attackers to decrypt passwords obtained with the attack described above in CVE-2024-3544. Sensitive information can be easily unencrypted by the attacker which could be used for arbitrary system command execution. This vulnerability has been closed by closing the CVE-2024-3544 vulnerability.

4

Issues Resolved

LM-5905	**Single Sign On**: "Login Failed Attempts" counter does not work in 7.2.54.8 and earlier releases. This issue has been fixed.
LM-5904	**GEO Clustering**: Fixed an internal issue that caused Cluster health checks to fail intermittently when the resource is available.
LM-5903	**Azure VLM Disk Space**: Fixed an issue that caused the */var/log/waagent* folder on an Azure VLM to run out of space.
LM-5902	**Single Sign On (NTLM Proxy)**: Fixed an issue that caused a user to be blocked incorrectly when the **Failed Login Attempts** parameter is set to 0.
LM-5901	**Single Sign On (NTLM/KCD)**: Fixed an issue that caused a user to be blocked incorrectly when the **Failed Login Attempts** parameter is set to 0.

5

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.