

LoadMaster 7.2.48.12 Release Notes

Generated on: 16 September 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

Best Practices Cipher Set 5

Supported Models for Upgrade 6

Upgrade Path 7

Upgrade Patch XML File Verification Notes 7

Chapter 3: Security Updates 8

Chapter 4: Existing Known Issues 9

1

Introduction

LMOS Version 7.2.48.12 is a security update of the Long Term Support (LTS) branch made available 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 LMOS release.

Related Links

- Best Practices Cipher Set
- Supported Models for Upgrade
- Upgrade Path

Best Practices Cipher Set

In LMOS 7.2.48.3, the **BestPractices** cipher set was updated. If you are upgrading from a version prior to 7.2.48.3, this change is effective immediately after upgrade to this release. This change was made to improve LoadMaster 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 upgrade 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.

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
	LM-4000		VLM-1000
	LM-5600		
	LM-8000		
	LM-8020		
	LM-8020M		

If your model number is not listed above, please see the list of End of Life models.

Upgrade Path

You can upgrade to this release of LMOS from any previous 7.2.x release. For full upgrade path information, please see the article Firmware Upgrade Path.

Related Links

- Upgrade Patch XML File Verification Notes

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'll need to 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 Kemp LoadMaster Firmware Upgrade Path article.
- LoadMasters 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.

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

Existing Known Issues

PD-13904	**SSO**: Password expiry notifications do not currently work with Forms Based Authentication (FBA) enabled on the server side.
PD-13873	**10 Gb Interfaces (AWS only)**: The AWS driver for 10 Gb interfaces (ENA) does not provide a link indication in its output, and so 'No Link' is the status displayed for a 10 Gb interface on AWS. Interface graphs for 10 Gb interfaces on the statistics page are not scaled properly, and so can run off the display; this will be addressed in a future release.
PD-13385	**WAF**: With WAF enabled on a Virtual Service, HTTP PUT commands that use chunked transfer encoding are dropped. This issue will be fixed in a future release.
PD-12838	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
PD-12653	**Networking**: A Hyper-V VLM will not boot when a 4th NIC is added.
PD-12616	**WAF / Compression**: With Web Application Firewall (WAF) enabled, compressed files are incorrectly decompressed. As a workaround, ensure compression is enabled in the Virtual Service Advanced Properties by selecting the **Enable Compression** option.
PD-12492	**Downgrade**: If an **Azure VLM** is downgraded to the LTS firmware release (7.1.35.x), the UI may display in the top right-hand corner that the VLM is a **Hyper-V VLM**. This indicates that the **Azure VLM Add-On Package** must be added to the system to provide full Azure VLM functionality. If this occurs, please contact Progress Kemp Support to get the required add-on package.
PD-12354	**Hardware Support**: The LoadMasters LM-X25 and LM-X40 do not support the following SFP+ modules in this release: LM-SFP-SX (SFP+ SX Transceiver 1000BASE-SX 850nm, 550m over MMF), LM-SFP-LX

	(SFP+ LX Transceiver 1000BASE-LX 1310nm, 10KM over SMF).
PD-12237	**HA / NTP**: Configuring NTP for the first time *after* the system is running in High Availability (HA) mode *and* when the current time on the machines is not correct, may cause the systems to both go into the Master state.
PD-12147	**ESP / RADIUS**: In a LoadMaster configuration with ESP and Radius server-side authentication enabled, sessions may fail to be established.
PD-12058	**Browser Support**: An issue exists when connecting to the LoadMaster UI when using newer versions of the Firefox browser on initial configuration of a hardware FIPS LoadMaster.
PD-11861	**RADIUS / IPv6**: IPv6 is not supported by the current RADIUS implementation in the LoadMaster for both WUI Authorization and ESP Authentication.
PD-11166	**Networking**: Azure LoadMasters are not translating the additional network address between the Master and Slave correctly.
PD-11044	**SharePoint Virtual Services**: A second authentication prompt is presented when a file is uploaded to SharePoint with the following configuration: WAF is configured with **Process Responses** enabled on the main Virtual Service and KCD is enabled on the SubVS level for server-side authentication.
PD-10917	**HA**: An issue exists when setting up a 2-armed HA Virtual LoadMaster in Azure.
PD-10784	**HA**: Configuring LoadMaster HA using eth1 on an Amazon Web Services (AWS) Virtual LoadMaster does not work.
PD-10586	**GEO**: If a GEO FQDN is configured with **All Available** as the **Selection Criteria**, IP addresses are returned even if the cluster is disabled.
PD-10490	**Content Rules**: The *vsremovewafrule* RESTful API command does not allow multiple rules to be removed.
PD-10474	**Intrusion Detection**: A SNORT rule is triggering a false positive in certain scenarios.
PD-10466	**Hardware Support**: The LoadMaster LM-X15 does not support the following SFP+ modules in this release: LM-SFP-SX (SFP+ SX Transceiver 1000BASE-SX 850nm, 550m over MMF), LM-SFP-LX (SFP+ LX Transceiver 1000Base-LX 1310nm, 10KM over SMF).
PD-10193	**Exchange 2010 Virtual Services**: A WAF, ESP, and KCD configuration with Microsoft Exchange 2010 is not supported.
PD-10188	**Browser Support**: (Safari) When adding a Real Server to a Virtual Service or SubVS using the Safari browser, the list of available Real Servers is not available.
PD-10159	**Statistics**: When upgrading firmware from version 7.1.35.*n*, CPU and network usage graphs are not appearing. As a workaround, reset the statistics in the WUI.
PD-10136	**Clustering**: In a LoadMaster cluster configuration, a new node can be added with the same IP address as an existing node.
PD-10129	**Virtual Services**: There is a discrepancy in validation between global-level connection timeout and Virtual Service-level timeout.

PD-9854, PD-13385	**WAF**: When WAF is enabled, any requests received that have chunked transfer encoding enabled (for example, POSTs) are not processed properly and are not forwarded to a real server.
PD-9816	**WAF**: There is an API command to list individual rules in a ruleset, but there is no command to list the available rulesets themselves.
PD-9765	**GEO**: DNS TCP requests from unknown sources are not supported.
PD-9507	**Networking**: Unable to add an SDN controller using the RESTful API/UI in a specific scenario.
PD-9476	**WAF**: There is no RESTful API command to get/list the installed custom rule data files.
PD-9375	**SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-8853	**GEO**: **Location Based** failover does not work as expected.
PD-8725	**GEO**: **Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.