Progress®
Kemp® LoadMaster®

LoadMaster Hotfix 7.2.48.9 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: Issues Resolved. 8

Chapter 4: Existing Known Issues 9

1

Introduction

LMOS Version 7.2.48.9 is a hotfix for a specific LoadMaster GEO issue and was made available on 3 February 2023. It is intended to be installed on a previous release of LMOS 7.2.48.x. Please read the sections below before installing this hotfix.

2

Before You Upgrade (READ ME FIRST)

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

Related Links

- Best Practices Cipher Set
- Supported Models for Upgrade
- Upgrade Path
- Upgrade Patch XML File Verification Notes

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 (e.g., SPLA, MELA) or platform (e.g., hardware, local cloud, public cloud).

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models
VLM-200	**LM-X1**	**LMB-1G**	**LM-2000**
VLM-500	**LM-X3**	**LMB-2G**	**LM-2200**
VLM-2000	**LM-X15**	**LMB-5G**	**LM-2400**
VLM-3000	**LM-X25**	**LMB-10G**	**LM-2500**
VLM-5000	**LM-X40**	**LMB-MAX**	**LM-2600**
VLM-10G	**LM-X40M**		**LM-3500**
VLM-GEO	**LM XHC 25G**		**LM-3600**
VLM-MAX	**LM XHC 40G**		**LM-5000**
VLM-SPLA-50	**LM XHC 100G**		**LM-5300**
VLM-SPLA-100	**LM-3000**		**LM-5500**
VLM-SPLA-500	**LM-3400**		**LM-Exchange**
VLM-SPLA-3000	**LM-4000**		**LM-GEO**
VLM-SPLA-GEO	**LM-5600**		**LM-UCS Series**
	LM-8000		**LM-R320**
	LM-8020		**LM-5400**
	LM-8020M		**LM-8020-FIPS**
			VLM-100
			VLM-1000

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 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 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 this 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

Issues Resolved

LM-1968	**GEO**: Fixed an issue where GEO system processes were exiting abnormally, possibly causing reboots, when DNS TSIG messages were received. Please note that LoadMaster does not support DNS TSIG messages, which fail with an appropriate error in the system log.

4

Existing Known Issues

The following issues appeared in the *Release Notes* for the previous release of LMOS.

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 on a SubVS.
PD-12653	**Networking**: A Hyper-V VLM won't 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 VS Advanced Properties by selecting the **Enable Compression** option.
PD-12492	**Downgrade**: If an **Azure VLM** is downgraded to the firmware version 7.1.35.x, the WUI 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 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 WUI 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-101	**Virtual Services**: There is a discrepancy in validation between global-level connection timeout and Virtual

29	Service-level timeout.
PD-9854, PD-13385	**WAF**: When WAF is enabled, any requests received that have chunked transfer encoding enabled (e.g., 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/WUI 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.