


# LoadMaster 7.2.59.4 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: Existing Known Issues . . . . . 9**

# 1

# Introduction

LMOS Version 7.2.59.4 is a security update of the General Availability (GA) 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 | | |

If your model number is not listed above, refer to 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 7.2.50.0 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 7.2.56.x and prior releases expired. For most customers, this will not impact normal operations, as explained in this article LoadMaster Code Signing Certificate Expires 27 May 2022.

All releases that occur after the above date (for example, LMOS 7.2.57.0) 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

# Existing Known Issues

| | |
|---|---|
| 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 the LoadMaster. |
| LM-2398 | **Kubernetes Ingress Controller (KIC)**: A real server deleted from the UI is not added back by KIC. |
| LM-2396 | **API**: On the KVM platform only, the *getall* API call fails. |
| LM-2034 | **GEO**: Starting with 7.2.55.0, using the **Real Server Load** selection criteria may result in no traffic being processed. |
| LM-1865 | **WAF Audit Logs**: No output is returned when selecting a date range. |
| LM-1809, LM-1800 | **Azure VLM**: Disk usage in the logging partition (*/var/log/*) may increase because of files used by the Azure agent (*waagent*) process that are never removed. Users who experience this issue will need to call support for a workaround. |
| LM-1557 | **Single Sign On**: A segmentation fault in the SSO management process can occur under high load resulting in users being logged out. Messages like the following will be seen in the log:<br>`kernel ssomgr[46119]: segfault at <num> ip <num> sp <num> error 4`<br>`kernel L7: verify_user: Auth request failed for id 0` |
| LM-152 | **GEO Cluster Checks**: GEO cluster checks against LoadMasters configured in Clustering mode do not |

| | |
|---|---|
| 7 | work. |
| LM-1412 | **API stats command**: On a unit in Clustering mode, the up/down status value returned by the stats command may be different (and incorrect) compared to the status returned by **listvs** or **vstotals**. |
| LM-1373 | **Let's Encrypt ACME Certificates**: After certificate renewal, the old certificate may still be in use by the Virtual Service. The workarounds are to either:<br>• Remove and re-add the Virtual Service certificate<br>• Disable and re-enable the Virtual Service |
| LM-1342 | **Kubernetes Ingress Controller**: Ingress may stop working if the default admin gateway is modified. The workaround is to return the setting to the old gateway address. |
| LM-1325 | **Let's Encrypt UI**: The UI for requesting a new certificate may not fully load with a large number of Virtual Services configured. The workaround is to use the API. |
| LM-477 | **GEO Downgrade**: When downgrading from a release that supports **more than 64 IPs per FQDN** to a release that only supports **up to 64 IPs per FQDN**, the GEO configuration may become corrupted if there is at least one FQDN in the configuration that contains more than 64 IP addresses. The corruption will likely be evidenced by errors in the UI/API when you list the FQDNs.<br>To avoid this issue entirely, reduce the number of IPs per FQDN to 64 or less for all FQDNs defined *before* you downgrade.<br>If you have already downgraded, you can switch back to the previous boot partition to go back to the newer release (which supports > 64 IPs per FQDN); you can then reduce the number of IPs as above and downgrade again.<br>If neither of these options is possible, contact Progress Kemp Support who will consult with engineering on a solution to your issues. |
| PD-19704 | **GEO Cluster Status**: When adding a Cluster that is unavailable (DOWN) to a Site, the Site may reflect the Cluster's status as available (UP) for a short time before changing to DOWN. |
| PD-19108, LM-127 | **GEO**: Modifying an FQDN entry displays a spurious error on the system console, similar to the one shown below. The FQDN is modified properly.<br><*FQDN*>:794 Uncaught ReferenceError: disp_addrr_elements is not defined<br>at <*FQDN*>:794<br>(anonymous) @ <*FQDN*>:794 |
| PD-19093, LM-127 | **GEO**: Cannot configure GEO into partnering mode unless there is at least one FQDN already defined. |
| PD-18646, LM-133 | **Certificate-Based Administrative Login**: Using a certificate that does not have a SAN attribute (that is, no Principal Name) results in a failed login attempt. |

| | |
|---|---|
| PD-18615, LM-134 | **GEO**: No statistics (queries per second, and so on) are displayed for a site if the FQDN is configured to use the "All Available" Selection Criteria. |
| PD-18099, LM-136 | **Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate. |
| PD-17927 | **LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI. |
| PD-15872 | **LDAP/Syslog**: StartTLS is not working when the **Server Certificate Validation** flag is enabled. |
| PD-15633 | **GEO**: If you add a Zone Name to GEO *after* you have 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. |
| PD-15475 | **VS Redirects**: If you attempt to upload a new redirect error HTML file to a Virtual Service with **Not Available Redirection Handling** enabled *while traffic is currently being redirected*, then traffic to the Virtual Service is dropped. Click the **Error Message** radio button in the UI and the Virtual Service begins accepting connections again. |
| PD-15354 | **SSO Timeout**: In LMOS 7.2.51.0, a fix was introduced for issues that caused an SSO client to not be properly logged out when the configured session timeout expires. It has been observed that while sessions do timeout, they are not always closed immediately upon the expiry of the timer; it can take close to a minute longer for the session to be closed. |
| PD-15294<br>LM-142 | **ESP Verify Bearer Header**: The LoadMaster does not return an error when an encrypted token is received and there is no SSL certificate assigned to the Virtual Service to decrypt the token. |
| PD-15172<br>LM-143 | **ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service. |
| PD-14943 | **Single Sign On**: When Form Based Authentication is enabled on the server side, it is possible that after filling out correct credentials and submitting the login form, the form will be presented again; once the second login form is submitted with correct credentials, the login succeeds. |
| PD-13899 | **ACLs and Real Servers**: Real Servers located on networks on which LoadMaster also has an IP address are *always* allowed to access Virtual Services on that network interface regardless of any access control list (ACL) settings on LoadMaster. For Layer 7 services, this issue can be worked around using Content Rules. The workaround for other services is to block access for local Real Servers (if desired) on another network device (firewall, switch, router, and so on). |
| PD-12838 | **ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS. |
| PD-126 | **WAF / Compression**: With Web Application Firewall (WAF) enabled, compressed files are incorrectly |

| | |
|---|---|
| 16 | decompressed. As a workaround, ensure compression is enabled in 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 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, contact Progress Kemp Support to get the required add-on package. |
| PD-12354, PD-10466 | **Hardware Support**: The LoadMaster models LM-X15, LM-X25, and LM-X40 do not support the following SFP+ modules: 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-111166 | **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-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 UI. |
| PD-10136 | **Clustering**: In a LoadMaster cluster configuration, a new node can be added with the same IP address as an existing node. |
| PD-9816, PD-9476 | **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-9375 | **SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication. |