

LoadMaster 7.2.54.4 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

Supported Models for Upgrade 6

Upgrade Path - Upgrade Patch XML File Verification Notes 7

Chapter 3: Security Updates - CVE-2022-0778 8

Chapter 4: Resolved Issues 9

Chapter 5: Existing Known Issues 10

1

Introduction

LMOS Version 7.2.54.4 is a security and stability release for the LMOS 7.2.54.x Long Term Support Feature (LTSF) branch, made available on 25 April 2022. This release addresses a security vulnerability in OpenSSL (CVE-2022-0778), as described under **Security Updates**, as well the additional fixes listed in the **Resolved Issues** section.

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

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

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

Upgrade Path - Upgrade Patch XML File Verification Notes

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.

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 - CVE-2022-0778

This patch updates LoadMaster's default OpenSSL libraries to Version 1.1.1n to address the OpenSSL security vulnerability described in CVE-2022-0778. In summary, this exploit leverages an internal OpenSSL bug that can cause an infinite loop to occur when parsing certificates. As a result, parsing a client certificate with an elliptic curve public certificate (or a public certificate with explicit elliptic curve parameters) may trigger the infinite loop and thus a denial of service attack. Further details are in the vulnerability database entry at the link above.

Note that this patch does *not* update the earlier version of OpenSSL present on LoadMaster (Version 1.0.2) to address CVE-2022-0778. This earlier OpenSSL version is used on LoadMaster only when the **Certificates & Security >SSL Options > OpenSSL Version** parameter is set to **Use older version**. If this is set to **Use current version** (the default value), then OpenSSL 1.1.1 is used.

Fortunately, with OpenSSL 1.0.2, there is no vulnerability to this exploit during the SSL handshake because of the handshake design in OpenSSL 1.0.2. On LoadMaster, the vulnerability can only be exploited by an administrative LoadMaster user who installs a specially crafted certificate and public key, and therefore presents a much lower risk of exposure to this vulnerability. This issue will be addressed in a future release.

4

Resolved Issues

LM-114	**GEO**: When GEO is running in Cloud High Availability (HA) Mode, DNS remains running on the standby unit as well as the active unit. This issue has been fixed.
LM-113	**Single Sign On - LDAP**: Fixed issues associated with LDAP SSO no longer working after an upgrade to LMOS 7.2.53. The issues appeared in conjunction with log messages like the following: ssomgr: ... Couldn't bind: [LDAP-AD] [*ip-addresses-omitted*]: 32, No such objectssomgr: do_sso_ldap_check: Could not get ldap_result for (*credentials-omitted*): 32 [No such object]
LM-108	**Caching**: Fixed an issue that caused expired cache entries to remain in the cache after the associated Virtual Service is stopped and restarted.
LM-86	**HTTP/2 and Chrome**: Fixed issues that could cause random client reconnect issues when accessing a website using the Chrome browser.
LM-85	**WAF / ESP**: Fixed an issue where modifying the WAF or ESP configuration of a Virtual Service can cause the LoadMaster to reboot.
LM-83	**Layer 7**: Fixed an internal issue that could cause memory exhaustion under very heavy load.

5

Existing Known Issues

PD-19496	**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.
PD-18099	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.
PD-18021	**Content Rule UI**: Display is incorrect when the 'Ignore case' option is enabled.
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 VS is dropped. Click the **Error Message** radio button in the UI and the VS 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	**ESP Verify Bearer Header**: LoadMaster does not return an error when an encrypted token is received and there is no SSL certificate assigned to the VS to decrypt the token.
PD-15172	**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, etc.).
PD-12838	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
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 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, please contact 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-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-109	**HA**: An issue exists when setting up a 2-armed HA Virtual LoadMaster in Azure.

17	
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-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-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.