Legacy GEO

Release Notes

UPDATED: 22 March 2021

Copyright Notices

Table of Contents

1 Legacy GEO Release Notes Introduction

This document describes the features added and issues resolved for legacy versions.

To see release notes for newer firmware versions, go to the **GEO Release Notes** section of the Kemp Documentation Page.

The GEO product is available in two forms:

- A standalone GEO product
- A Global Sever Load Balancing (GSLB) Feature Pack that is part of the Kemp load balancer (LoadMaster) product

> This document applies to both forms of GEO. We recommend making a full back up of the LoadMaster configuration before upgrading the software.

> Installation of this software and reloading of the configuration may take up to five minutes, or possibly more, during which time the LoadMaster being upgraded is unavailable to carry traffic.

1.1 Prerequisites

The following are recommendations for upgrading the software:

- The person undertaking the upgrade should be a network administrator or someone with equivalent knowledge
- In case of issues restoring backup configurations, configuring LoadMaster or other maintenance issues, please refer to the LoadMaster documentation which can be found at https://kemptechnologies.com/documentation

1.2 Support

If there are problems loading the software release, please contact Kemp support staff using our website and a Kemp support Engineer will call you promptly.

1.3 Compatible Products

- GEO standalone product
- LoadMaster with the Global Server Load Balancer (GSLB) Feature Pack

2 Release 2.2.35.5/7.1.35.5

Refer to the sections below for details about firmware version 2.2.35.5/7.1.35.5. This was released on 22nd March 2018.

2.1 2.2.35.5/7.1.35.5 - Issues Resolved

PD-11023	Previously, a critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Now, this vulnerability has been mitigated against with more stringent security checks. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

2.2 2.2.35.5/7.1.35.5 - Known Issues

PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.

3 Release 7.1.35.4

Refer to the sections below for details about firmware version 7.1.35.4. This was released on 2nd August 2017.

3.1 2.2.35.4/7.1.35.4 - Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do no work with IPv6 source addresses.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter vales for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.

4 Release 2.2.35.3/7.1.35.3

Refer to the sections below for details about firmware version 2.3.35.3/7.1.35.3. This was released on 5th April 2017.

4.1 Feature Enhancements

- Updated BIND to version 9.10.4-P5 to mitigate against the following vulnerabilities:
  - CVE-2016-9131
  - CVE-2016-9147
  - CVE-2016-9444
  - CVE-2016-9778

4.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do no work with IPv6 source addresses.

5 Release 2.2.35/7.1.35

Refer to the sections below for details about firmware version 2.2.35/7.1.35. This was released on 2nd August 2016.

5.1 New Features

- GEO now supports blacklists.
- GEO per-FQDN settings.
- Enhanced GEO health checks to allow grouping by cluster.

5.2 Issues Resolved

PD-7225	The **listcustomlocation** API command is now showing the correct custom locations which have been added.
PD-7134	Fixed the GEO LoadMaster WUI to display missing menu elements.
PD-7481	Fixed an issue relating to incorrect site selection failover when using **Location Based** as the **Selection Criteria**.

5.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do no work with IPv6 source addresses.

PD-7770	There are some issues with the GEO proximity **Selection Criteria**.
PD-7516	The GEO Location Based option for “Everywhere” cannot be set and is not listed in the API.
PD-7338	The **listclusters** API command returns 0 as the **CheckerPort** value if the checker is set to **tcp**. The default value when using TCP health checks is 80 and that should be returned.
PD-7522	If a GEO map is modified using the API and the IP address for the site is not specified, nothing is returned (an error should be displayed).

6 Release 2.2.34.1/7.1.34.1

Refer to the sections below for details about firmware version 2.2.34.1/7.1.34.1. This was released on 18th May 2016.

6.1 Feature Enhancements

- It is now possible to delete custom GEO locations.
- PowerShell and Java API commands have been added for adding custom locations to FQDNs.

6.2 Issues Resolved

PD-6657	Fixed an issue relating to Private/Public site preference with proximity selection.
PD-6641	Fixed a display issue for sites using a built-in geographic location database.
PD-6626	Fixed geographic coordinate resolution of existing sites when switching to proximity selection.
PD-6215	Added API commands to allow public IP addresses to be treated as private on GEO.

6.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-7225	The **listcustomlocation** API command shows custom locations that have not been added.

7 Release 2.2-32a/7.1-32a

Refer to the sections below for details about firmware version 2.2-32a/7.1-32a. This was released on 26th January 2016.

7.1 Issues Resolved

PD-6514	Fixed an issue relating to site restrictions for FQDNs.
PD-6476	Improved GEO proximity stability.
PD-6095	Fixed an issue with the add/remove country and change map location API commands for GEO.
PD-6078	It is now possible to add a custom location to an IP in an FQDN using API commands.
PD-5915	Fixed an issue which was preventing an extra name server from being added.
PD-3642	Fixed an issue relating to GEO Weighted Round Robin statistics.

7.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-6626	Changing an existing FQDN with sites to proximity balancing causes automatic resolution to fail.
PD-6627	If 'bad data' is entered in the coordinates of an FQDN, automatic resolution will fail.

8 Release 2.2-30/7.1-30

Refer to the sections below for details about firmware version 2.2-30/7.1-30. This was released on 3rd November 2015.

8.1 Feature Enhancements

- There is now further flexibility in GEO around selectively responding with public or private sites based on whether a client is from a public or private IP address.
- Enhancements have been made to the GEO partner status indicators.

8.2 Issues Resolved

PD-5478	Fixed an issue with the GEO round robin scheduling method for IPv6.
PD-5282	Fixed an issue relating to the GEO proximity scheduling method.
PD-4863	Fixed an issue which was preventing GEO custom locations from being edited.
PD-5853	Fixed an issue relating to GEO health checking.

8.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-5582	There are some GEO issues relating to the resource check parameters and cluster health checking.
PD-5915	In GEO, it is not possible to add multiple name servers using the WUI. This can be done in the API as a workaround.

9 Release 2.2-28b/7.1-28b

Refer to the sections below for details about firmware version 2.2-28b/7.1-28b. This was released on 28th August 2015.

9.1 Feature Enhancements

- Updated firmware to mitigate against CVE-2015-5477 vulnerability.

9.2 Issues Resolved

PD-5581	Fixed a GEO Web User Interface (WUI) issue which caused issues with multiple locations being assigned.

9.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.
PD-4863	Custom locations on the LoadMaster GEO cannot be disabled.

10 Release 2.2-28a/7.1-28a

Refer to the sections below for details about firmware version 2.2-28a/7.1-28a. This was released on 29th July 2015.

10.1 Issues Resolved

PD-5251	Fixed an issue which prevented some GEO miscellaneous parameters to be set.

10.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.

11 Release 2.2-28/7.1-28

Refer to the sections below for details about firmware version 2.2-28/7.1-28. This was released on 24th June 2015.

11.1 Feature Enhancements

- Removed superfluous messages in GEO logging.
- Added status indicators for partner SSH tunnels.

11.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

12 Release 2.2-26/7.1-26

Refer to the sections below for details about firmware version 2.2-26/7.1-26. This was released on 1st May 2015.

12.1 Feature Enhancements

- New LoadMaster installations now come pre-installed with an up-to-date GEO database, including IPv6.
- Improved GEO partner IP entry method - only the shared IP address needs to be entered into the **Remote GEO LoadMaster Access** text box for HA configurations.

12.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

13 Release 2.2-24a/7.1-24a

Refer to the sections below for details about firmware version 2.2-24a/7.1-24a. This was released on 11th February 2015.

13.1 Feature Enhancements

- Added new GEO cluster RESTful API commands which list and show clusters.

13.2 Issues Resolved

PD-3344	SSH can now be disabled on a GEO cluster to increase security.
PD-3319	Alternate gateway support has been added for GEO LoadMasters with multiple interfaces.
PD-3160	Fixed a problem with the **modmap** RESTful API command.
PD-3104	The **addmap** RESTful API command now works in all scenarios.
PD-3075	A superfluous error message, which displayed when setting the **isolateips** parameter using the **ModifyFQDN** command, has been removed.

13.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

14 Release 2.2-22b/7.1-22b

Refer to the sections below for details about firmware version 2.2-22b/7.1-22b. This was released on 3rd December 2015.

14.1 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3160	There is a bug with the **modmap** RESTful API command.
PD-3104	The **addmap** RESTful API command does not work when the **Selection Criteria** is set to **Real Server Load**.
PD-3075	A superfluous error message appears when you attempt to set the **isolateips** parameter using the PowerShell **ModifyFQDN** command.

15 Release 2.2-22/7.1-22

Refer to the sections below for details about firmware version 2.2-22/7.1-22. This was released on 25th November 2014.

15.1 Feature Enhancements

- Security enhancements have been made to GEO.
- Multiple Virtual Services with the same IP address can now be added to the GEO Real Server Load Cluster Check.
- Updated the BIND version to 9.9.6-ESV to address CVE-1999-0662.

15.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3160	There is a bug with the **modmap** RESTful API command.
PD-3104	The **addmap** RESTful API command does not work when the **Selection Criteria** is set to **Real Server Load**.
PD-3075	A superfluous error message appears when you attempt to set the **isolateips** parameter using the PowerShell **ModifyFQDN** command.

16 Release 2.2-20/7.1-20

16.1 New Features

- The ability to designate GEO listening interfaces.
- The ability to use multiple interfaces to listen for GEO requests.

16.2 Feature Enhancements

- GEO API commands have been added.

16.3 Issues Resolved

PD-2644	Fixed an issue with syncing some GEO settings.

16.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

17 Release 2.2-18b/7.1-18b

17.1 New Features

- GEO enhancements

New GEO features which allow failover and isolates public/private sites. Also, two GEO selection criteria options have been renamed to more appropriately reflect their functions (**Location Based** has been renamed to **Proximity** and **Regional** has been renamed to **Location Based**).

17.2 Issues Resolved

PD-1941	Removed unnecessary options for GEO cluster synchronization

17.3 Known Issues

- A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- GEO health check intervals do not match the settings configured

18 Release 2.2-16/7.1-16

18.1 New Features

- The LoadMaster GEO Operating System is now running on Linux kernel 3.10.28

18.2 Issues Resolved

PD-1687	Made the GEO sync mechanism more tolerant of rapid changes

18.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

19 Release 2.1.14/7.0-14

19.1 Feature Enhancements

- GEO can now be disabled and enabled using the Web User Interface (WUI) (when GEO is disabled it is possible to modify the packet filter settings)

19.2 Issues Resolved

PD-1145	DNS requests can now be made to the LoadMaster GEO over an IPv6 network
PD-1277	BIND has been updated to version 9.6-ESV-R10-P2

19.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

20 Release 2.1.12a/7.0-12a

20.1 Feature Enhancements

- GEO search order changed

20.2 Issues Resolved

PD-771	Fixed issue where the site failure and recovery settings were not updating to the partner
PD-808	Fixed issue where the FQDN was not updating to the partner

20.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

21 Release 2.1.10/7.0-10

21.1 Known Issues

- A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Site failure and recovery settings are not replicated to the partner GEO.
- In some cases, FQDNs are not replicated to the partner GEO.

22 Release 2.1.8e/7.0-8e

22.1 Feature Enhancements

- Automated Licensing and Support Infrastructure (ALSI) Enhancements

22.2 Issues Resolved

PD-700	Fixed reboot issue when changing service types

22.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

23 Release 2.1.8/7.0-8

23.1 New Features

- IP Range Selection Criteria
- Certificates Functionality

23.2 Issues Resolved

PD-392	Issue with GEO sync has been resolved

23.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

Last Updated Date

This document was last updated on 22 March 2021.