Release Notes for Cisco Prime LAN Management Solution 4.2.4

November 2013, OL-25950-04

Contents

These Release Notes provide instructions for downloading and installing Cisco Prime LAN Management Solution (LMS) 4.2.4. This document also points you to the known problems in LMS 4.2.4.

This document has the following sections:

- Introduction
- What's New in This Release
- Syslog-ng Support
- System and Browser Requirements for Server and Client
- Java Plug-in version for Cisco Prime LAN Management Solution 4.2.4
- Downloading Cisco Prime LAN Management Solution 4.2.4
- Installing Cisco Prime LAN Management Solution 4.2.4
- Upgrading to Cisco Prime LAN Management Solution 4.2.4
- Bugs
- Product Documentation
- Related Documentation
- Obtaining Documentation, Obtaining Support, and Security Guidelines
- Notices

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco Prime LAN Management Solution provides powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. It also supports Cisco technologies such as Identity, EnergyWise, Auto Smartports, and Smart Install.

What's New in This Release

This section explains the new PSIRT Policies in LMS 4.2.4:

PSIRT Policies

PSIRT Policy Group supports the following policies:

- IOS Software DHCPv6 DoS Vulnerability - 20120926
- IOS Software Malformed BGP Vulnerability - 20120926
- IOS Software SIP DoS Vulnerability - 20120926
- IOS Software DHCP DoS Vulnerability - 20120926
- IOS Software NAT For SIP DoS Vulnerability - 20120926
- IOS Software NAT DoS Vulnerability - 20120926
- IOS Software IPS DoS Vulnerability - 20120926
- IOS Software Smart Install DoS Vulnerability - 20120328
- IOS Software Reverse SSH DoS Vulnerability - 20120328
- IOS Software Multicast Source Discovery Protocol Vulnerability - 20120328
- IOS Internet Key Exchange Vulnerability - 20120328
- IOS Software MACE DoS Vulnerability - 20120328
- IOS Software WAAS DoS Vulnerability - 20120328
- IOS Software Memory Leak Associated with Crafted IP Packets Vulnerability - 20120328
- IOS Software Memory Leak in HTTP Inspection Vulnerability - 20120328
- IOS Software Memory Leak in H.323 Inspection Vulnerability - 20120328
- IOS Software Memory Leak in SIP Inspection Vulnerability - 201203288
- IOS Software Command Authorization Bypass Vulnerability - 201203284
- IOS Software NAT SIP Memory Starvation Vulnerability - 20120328
- IOS Software RSVP Denial of Service Vulnerability - 20120328
- ASA DHCP Memory Allocation Denial of Service Vulnerability - 20121010
- ASA SSL VPN Authentication Denial of Service Vulnerability - 20121010
- ASA SIP Inspection Media Update Denial of Service Vulnerability - 20121010
- ASA DCERPC Inspection Buffer Overflow Vulnerability - 20121010
- ASA Two DCERPC Inspection Denial Of Service Vulnerability - 20121010
- ASA Denial of Service Vulnerability - 20120620

- IOS Software Tunneled Traffic Queue Wedge Vulnerability - 20120926

IOS Software DHCPv6 DoS Vulnerability - 20120926

Description

Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Malformed BGP Vulnerability - 20120926

Description

Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability.This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software SIP DoS Vulnerability - 20120926

Description

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software DHCP DoS Vulnerability - 20120926

Description

Cisco IOS Software contains a vulnerability that could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software NAT For SIP DoS Vulnerability - 20120926

Description

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software NAT DoS Vulnerability - 20120926

Description

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software IPS DoS Vulnerability - 20120926

Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ios-ips

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Smart Install DoS Vulnerability - 20120328

Description

Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Reverse SSH DoS Vulnerability - 20120328

Description

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Multicast Source Discovery Protocol Vulnerability - 20120328

Description

A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Internet Key Exchange Vulnerability - 20120328

Description

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software MACE DoS Vulnerability - 20120328

Description

Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software WAAS DoS Vulnerability - 20120328

Description

Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

Applicable Platforms

Cisco IOS Devices.

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Memory Leak Associated with Crafted IP Packets Vulnerability - 20120328

Description

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Memory Leak in HTTP Inspection Vulnerability - 20120328

Description

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Memory Leak in H.323 Inspection Vulnerability - 20120328

Description

The Cisco IOS Software contains Memory Leak in H.323 Inspections. Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection

- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Memory Leak in SIP Inspection Vulnerability - 20120328

Description

The Cisco IOS Software contains Memory Leak in SIP Inspections. Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Command Authorization Bypass Vulnerability - 201203284

Description

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities. The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software NAT SIP Memory Starvation Vulnerability - 20120328

Description

The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

Cisco has released free software updates that address this vulnerability. A workaround is available to mitigate the vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software RSVP Denial of Service Vulnerability - 20120328

Description

Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

Cisco has released free software updates that address this vulnerability. A workaround is available to mitigate this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120328 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA DHCP Memory Allocation Denial of Service Vulnerability - 20121010

Description

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) may be affected by the following vulnerability:

DHCP Memory Allocation Denial of Service Vulnerability

Successful exploitation of any of these vulnerabilities could allow an unauthenticated remote attacker to trigger a reload of the affected device. Exploitation of the DCERPC Inspection Buffer Overflow Vulnerability could additionally cause a stack overflow and possibly the execution of arbitrary commands. Cisco has released free software updates that address these vulnerabilities. Workarounds are available for some of these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20121010 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA SSL VPN Authentication Denial of Service Vulnerability - 20121010

Description

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) may be affected by the following vulnerability:

SSL VPN Authentication Denial of Service Vulnerability

Successful exploitation of any of these vulnerabilities could allow an unauthenticated remote attacker to trigger a reload of the affected device. Exploitation of the DCERPC Inspection Buffer Overflow Vulnerability could additionally cause a stack overflow and possibly the execution of arbitrary commands. Cisco has released free software updates that address these vulnerabilities. Workarounds are available for some of these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20121010 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA SIP Inspection Media Update Denial of Service Vulnerability - 20121010

Description

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) may be affected by the following vulnerability:

SIP Inspection Media Update Denial of Service Vulnerability

Successful exploitation of any of these vulnerabilities could allow an unauthenticated remote attacker to trigger a reload of the affected device. Exploitation of the DCERPC Inspection Buffer Overflow Vulnerability could additionally cause a stack overflow and possibly the execution of arbitrary commands. Cisco has released free software updates that address these vulnerabilities. Workarounds are available for some of these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20121010 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA DCERPC Inspection Buffer Overflow Vulnerability - 20121010

Description

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) may be affected by the following vulnerability:

DCERPC Inspection Buffer Overflow Vulnerability

Successful exploitation of any of these vulnerabilities could allow an unauthenticated remote attacker to trigger a reload of the affected device. Exploitation of the DCERPC Inspection Buffer Overflow Vulnerability could additionally cause a stack overflow and possibly the execution of arbitrary commands. Cisco has released free software updates that address these vulnerabilities. Workarounds are available for some of these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20121010 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA Two DCERPC Inspection Denial Of Service Vulnerability - 20121010

Description

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) may be affected by the following vulnerability:

Two DCERPC Inspection Denial Of Service Vulnerability

Successful exploitation of any of these vulnerabilities could allow an unauthenticated remote attacker to trigger a reload of the affected device. Exploitation of the DCERPC Inspection Buffer Overflow Vulnerability could additionally cause a stack overflow and possibly the execution of arbitrary commands. Cisco has released free software updates that address these vulnerabilities. Workarounds are available for some of these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20121010 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

ASA Denial of Service Vulnerability - 20120620

Description

Cisco ASA 5500 Series Adaptive Security Appliances (Cisco ASA) contain a vulnerability that may allow an unauthenticated, remote attacker to cause the reload of the affected device.

Cisco has released free software updates that address this vulnerability. Workarounds are available to mitigate this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaipv6

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (20120620 of 1.0)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

IOS Software Tunneled Traffic Queue Wedge Vulnerability - 20120926

Description

Cisco IOS Software running on the Cisco 10000 Series router has been demonstrated to be affected. Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-c10k-tunnels

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (20120926 of 1.1)

Security advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security notices are provided for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Syslog-ng Support

This section includes the following topics:

- Overview
- Installing Syslog-ng
- Sample Reference Configuration File
- Restarting from GUI
- Restarting from CLI

Overview

Syslog-ng is an open source implementation of the syslog protocol for UNIX and UNIX-like systems.It extends the original syslog model with content-based filtering, rich filtering capabilities, and flexible Configuration options and adds important features to syslog, such as using TCP for transport.

Syslog-ng is running on the same server as the LMS box. Syslogs are being written to a file for example /var/log/Syslog_info from which LMS can be read and this method is easier to implement.

Installing Syslog-ng

To install Syslog-ng on Linux/Solaris server follow the steps given below:

Step 1 Install the entire syslog-ng prerequisites. For more information refer Syslog-ng Administrator Guide by navigating to the path **Support -> Documentation** in the link http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/compiling/

Step 2 Download the latest version of syslog-ng OSE from the BalaBit link.The installable is available as a tar.gz archive file.

Step 3 Download the latest version of the EventLog library from the BalaBit link.

Step 4 Uncompress the eventlog archive using the following commands to create a new directory containing the source code of eventlog:

 # tar xvfz eventlog-x.x.x.x.tar.gz

or the

 # gunzip -c eventlog-x.x.x.x.tar.gz | tar xvf -

Step 5 Enter the following command to add the new directory to pkgconfig directory

PKG_CONFIG_PATH=/usr/local/lib/pkgconfig:#PKG_CONFIG_PATH

Note By default, eventlog creates a file used by the syslog-ng configure script in the /usr/local/lib/pkgconfig directory.

Step 6 Go to the created directory and enter the following commands:

 # ./configure

 # make

 # make install

Step 7 Uncompress the syslog-ng archive using the following commands to create a new directory containing the source code of syslog-ng.

tar xvfz syslog-ng-x.xx.tar.gz

or the

unzip -c syslog-ng-x.xx.tar.gz | tar xvf -

Step 8 Go to the created directory and enter the following commands to build Syslog-ng using default options:

 # ./configure

 # make

 # make install

Sample Reference Configuration File

Given below is a sample configuration file that is used to get a quick jump start. User is need to modify the IP address, ports, and other such local information according to the environment.

Syslog-ng.conf file located by default on /usr/local/etc

```
############################################################
# First, set some global options.
options {
use_fqdn(no);
use_dns(no);
long_hostnames(off);
sync(0);
};
# Then, set some global sources.
source src {
udp(ip("0.0.0.0") port(514));
};
# Then, set some global destinations.
destination Remote_LMS_SyslogNG {
udp("192.168.141.43" port(514) spoof_source(yes));
};
destination Local_LMS_SyslogNG {
file("/var/log/syslogs_info"
template("$DATE $HOST $MSG\n")
);
};
# Now log it
log {
source(src);
if using Remote LMS, uncomment the following:
# destination(Remote_LMS_SyslogNG);
if running SyslogNG Locally on LMS, uncomment the following:
```

 # destination(Local_LMS_SyslogNG);

};

##

Syslog-NG process must be restarted on changing the Conf file using the following commands:

/etc/init.d/syslog-ng stop

/etc/init.d/syslog-ng start

To verify Syslog-ng processs use the command **/etc/init.d/syslog-ng status.**

Note For using Remote Syslog-ng, use the command **destination(Remote_LMS_SyslogNG)** and use LMS server IP addresss as the Remote server. For using Remote LMS, uncomment the line **#destination(Remote_LMS_SyslogNG**). Remote Syslog-ng will be certified from LMS 4.2.5 onwards.

Note For using Syslog-ng locally on LMS, use the command **destination(Local_LMS_SyslogNG)** and uncomment the line **# destination(Local_LMS_SyslogNG).**

SyslogAnalyzer and Collector process must be restarted on LMS Server.

Restarting from GUI

To restart SyslogAnalyzer and Collector process from GUI follow the steps given below:

Step 1 Login to LMS Server using login credentials.

Step 2 Navigate to **Admin -> System-> Server Monitoring > Processes**.

Step 3 Look for SyslogAnalyzer and Collector process, check that row, and click Stop.

Step 4 Once the process is stopped, check the same row (if unchecked), and click Start.

Restarting from CLI

To restart SyslogAnalyzer and Collector process using the command-line interface (CLI).

Linux/Solaris:

To stop SyslogAnalyzer and Collector process, enter the following command:

 # /opt/CSCOpx/bin/pdterm SyslogCollector SyslogAnalyzer

To start SyslogAnalyzer and Collector process, enter the following command:

 # /opt/CSCOpx/bin/pdexec SyslogCollector SyslogAnalyzer

To verify SyslogAnalyzer and Collector process, enter the following command:

 # /opt/CSCOpx/bin/pdshow SyslogCollector SyslogAnalyzer

For any Support related to Syslog-ng, please refer to Syslog-ng Support Forum: https://lists.balabit.hu/mailman/listinfo/syslog-ng

Note Syslog-ng version 3.x.x is certified in Linux Server where LMS 4.2.4 and Syslog-ng is running on the same server.

System and Browser Requirements for Server and Client

Before you begin to install LMS software, you must check if your system meets the recommended prerequisites.

The recommended LMS 4.2.4 server and client requirements on the supported operating systems are based on the license that you use on a single server or multi-server setup. For more information, see System and Browser Requirements for Server and Client in *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*.

Note The browsers additionally supported in LMS 4.2.4 are Mozilla Firefox 19.0 and ESR 17.

Note LMS 4.2.4 supports VMware ESXi Server 5.1.

Java Plug-in version for Cisco Prime LAN Management Solution 4.2.4

LMS 4.2.4 supports Java Plug-in version 1.7.0_21 for accessing Cisco Prime applications such as Topology Services on Windows XP Service Pack 3, Windows 2008, Windows 2008 R2 and Windows 7.

Downloading Cisco Prime LAN Management Solution 4.2.4

You can download LMS 4.2.4 either from Cisco.com or as a Software Update from:

Admin > System > Software Center > Software Update

This section contains:

- Downloading from Cisco.com
- Downloading from Software Center

Downloading from Cisco.com

LMS 4.2.4 is available on Cisco.com. To download LMS 4.2.4:

Step 1 Go to the Download Software page http://www.cisco.com/cisco/software/type.html?mdfid=284259296&flowid=31102&softwareid=280775102.

Step 2 Based on the preferred operating system, choose one of the following from the software download page:

- Solaris
- Soft Appliance
- Windows

Step 3 Download the LMS 4.2.4 software zip file into a directory on your system.

Step 4 Check the checksum value of the downloaded files with the values given below:

- Checksum value for Solaris—3298977572 1288946759
- Checksum value for Soft Appliance—3154292267 1198937541
- Checksum value for Windows—1072086312 1186440168

Downloading from Software Center

You can use the Software Update function in LMS Software Center to download LMS 4.2.4.

To download LMS 4.2.4 from the Software Center:

Step 1 Go to the Cisco Prime home page and choose **Admin > System > Software Center > Software Update**.

The Software Updates page appears.

Step 2 In the Products Installed table, check the check box corresponding to LAN Management Solution.

Step 3 Click either:

- **Download Updates**. See Using the Download Updates Option.

  Or

- **Select Updates**. See Using the Select Updates Option.

Using the Download Updates Option

To download LMS 4.2.4 using the Download Updates option:

Step 1 Click **Download Updates** on the Software Updates page.

The Cisco.com and Proxy Server Credentials dialog box appears.

Step 2 Enter your Cisco.com username and password. Both are mandatory.

If you have configured proxy settings under **Admin > System > Cisco.com Settings > Proxy Server Setup**, enter the Proxy server user name and password.

Step 3 Click **Next**.

The Destination Location page appears. The destination location should not be the location where Cisco Prime LMS is installed.

The default download directory is:

/opt/psu_download—On Solaris

/opt/psu_download—On Soft Appliance

System Drive:\psu_download—On Windows

Software Center does not support downloading software or device updates into the same directory where you have installed Cisco Prime LAN Management Solution, or any of its sub-directories. Also, you cannot download software or device updates under System directories.

Step 4 Enter the location, or browse to the location using the Browse tab.

The destination location must have casuser write permissions.

Step 5 Click **Next**.

The Summary page appears with a summary of your inputs.

Step 6 Click **Finish** to confirm the download operation.

Using the Select Updates Option

To download LMS 4.2.4 using the Select Updates option:

Step 1 Click **Select Updates** in the Software Updates page.

The Cisco.com and Proxy Server Credentials dialog box appears.

Step 2 Enter your Cisco.com username and password. Both are mandatory.

If you have configured proxy settings under **Admin > System > Cisco.com Settings > Proxy Server Setup**, enter the Proxy server username and password.

The Available Images page appears.

Step 3 Do either of the following:

- Select the lms4_2_4_sol_k9.zip file for Solaris.
- Select the lms4_2_4_lnx_k9.zip file for Soft Appliance
- Select the lms4_2_4_win_k9.zip file for Windows.

Step 4 Click **Next**.

The Destination Location page appears. The destination location should not be the location where Cisco Prime is installed.

The default download directory is:

/opt/psu_download—On Solaris

/opt/psu_download—On Soft Appliance

System Drive:\psu_download—On Windows

Software Center does not support downloading software or device updates into the same directory where you have installed Cisco Prime LAN Management Solution, or any of its sub-directories. Also, you cannot download software or device updates under System directories.

Step 5 Enter the location, or browse to the location using the Browse tab.

The destination location must have casuser write permissions.

Step 6 Click **Next**.

The Summary page appears with a summary of your inputs.

Step 7 Click **Finish** to confirm the download operation.

Installing Cisco Prime LAN Management Solution 4.2.4

This section describes the procedure to install Cisco Prime LMS 4.2.4 on Solaris, Soft Appliance, and Windows systems.

The LMS 4.2.4 installation program takes approximately 50 minutes to complete on Windows, Soft Appliance and Solaris, on a single server with the recommended hardware requirements.

This can take more than two hours if you perform network management integration while installing.

- If Virus Check is enabled in your system, then installation of LMS 4.2.4 will take a longer time.
- If HP Openview or Netview is running on your system, installation will take a longer time. Stop these services to do a faster installation.

This section contains:

- Prerequisites for Installing Cisco Prime LMS 4.2.4 Software
- Installing LMS 4.2.4 on Solaris
- Installing LMS 4.2.4 on Soft Appliance
- Installing LMS 4.2.4 on Windows
- Re-installing LMS 4.2.4
- Remote Upgrade to LMS 4.2.4

Prerequisites for Installing Cisco Prime LMS 4.2.4 Software

Cisco Prime LMS 4.2.4 installation must be performed in the following order on LMS 4.2:

- LMS 4.2 -> LMS 4.2.2 -> LMS 4.2.4
- LMS 4.2 -> LMS 4.2.2 -> LMS 4.2.3 -> LMS 4.2.4
- LMS 4.2 -> LMS 4.2.1 -> LMS 4.2.2 -> LMS 4.2.3 -> LMS 4.2.4. For more details, see Prerequisites in *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*.

Installing LMS 4.2.4 on Solaris

To install LMS 4.2.4 on a Solaris system:

Step 1 Navigate to the location where you have downloaded the lms4_2_4_sol_k9.zip file in your system.

Note We recommend that you run the installation from a local hard drive to avoid errors that may result from the network being slow or busy.

Step 2 Copy the downloaded software image to a directory having a minimum of 10 GB free space.

Step 3 Unzip the lms4_2_4_sol_k9.zip file.

The contents of the zip file are extracted under the lms4_2_4_sol_k9 directory.

Step 4 Navigate to the lms4_2_4_sol_k9 folder.

Step 5 Run the installation setup script by entering:

```
# sh setup.sh
```

or

```
# ./setup.sh
```

A Welcome message appears:

```
Welcome to Cisco Prime LAN Management Solution 4.2.4 setup program.
```

A prompt appears:

```
Press Enter to read/browse the following license agreement:
```

Step 6 Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
Do you accept all the terms of the License Agreement? (y/n) [n]:
```

Step 7 Enter **Y** to accept the license agreement and proceed with the installation, or enter **N** to deny and quit the installation.

While installing from the network drive, the Installing from Network Drive message appears.

Installation from the network drive will be slower than installing from the local drive.

Step 8 Enter **Y** to proceed or **N** to exit installation.

If you enter **Y**, then the following warning message appears:

```
WARNING: Automatic data backup does not happen during this installation. We recommend you
to take a backup of data before starting this installation.
```

Step 9 Enter **Y** to proceed or **N** to exit installation.

If you enter **Y**, then the following warning messages appear to inform you to install the Cluster Patches required for Solaris 10:

```
WARNING: Ensure that you have installed the recommended Solaris 10 cluster patches
released on Apr/17/07, in this server.

WARNING: If these cluster patches are not installed, please download and install them
from http://www.oracle.com/us/sun/index.htm.

WARNING: Otherwise, some features of the Cisco Prime applications will not function
properly.

Do you want to continue the installation? (y/n) [y]:
```

Step 10 Enter **Y** to proceed with the installation.

A list of other warning messages appears finally before the installation completes successfully.

Installing LMS 4.2.4 on Soft Appliance

To install LMS 4.2.4 on Soft Appliance:

Step 1 Log into the shell and navigate to the location where the upgrade file, lms4_2_4_lnx_k9.zip is stored.

```
myhost/admin# shell
starting shell…
[myhost/ root-ade ~]
```


Note The login name that appears in the command prompt depends on the login name entered by the user while installing LMS on VM Console.

Step 2 Unzip the lms4_2_4_lnx_k9.zip file to extract Cisco_Prime_LAN_Management_Solution_4_2_4.tar.gz.

```
[myhost/ root-ade myloc] unzip lms4_2_2_lnx_k9.zip
```

Step 3 Copy the Cisco_Prime_LAN_Management_Solution_4_2_4.tar.gz to local disk partition of LMS 4.2.3/LMS 4.2.2 installed server (/localdisk).

Step 4 Log in with your credentials to the VM Console through Vsphere client.

Step 5 Create either a local or remote repository. A repository contains URL and credential details

```
myhost/admin# configure terminal
myhost/admin(config)# repository <<myrepo>>
myhost/admin(config-Repository)# url ?
<WORD>  Enter repository URL, including server and path info (Max Size - 80)
cdrom:  Local CD-ROM drive (read only)
disk:   Local storage
ftp:    URL using a FTP server
http:   URL using a HTTP server (read only)
https:  URL using a HTTPS server (read only)
nfs:    URL using a NFS server
sftp:   URL using a SFTP server
tftp:   URL using a TFTP server
```

Step 6 Combine the URL to the repository that uses a local or remote storage.

a. The following IOS CLI shows how to combine the URL to a repository that uses a local storage:

```
myhost/admin(config-Repository)# url disk:
myhost/admin(config-Repository)# exit
myhost/admin(config)# exit
myhost/admin# write mem
Generating configuration...
myhost/admin#
```

b. The following IOS CLI shows how to combine the URL to a repository that uses an anonymous FTP server:

```
myhost/admin(config-Repository)# url ftp://<<ftp_location>>
myhost/admin(config-Repository)# user <<ftp_username>> password plain
<<ftp_password>>
myhost/admin(config-Repository)# exit
```

```
myhost/admin(config)# exit
myhost/admin# write mem
Generating configuration...
myhost/admin#
```

You can use the above mentioned steps for other protocols.

Step 7 Run the below command in the VM console in VSphere client.

```
myhost/admin# application upgrade Cisco_Prime_LAN_Management_Solution_4_2_4.tar.gz
<<myrepo>>
Save the ADE-OS running configuration? (yes/no) [yes]?
```

Step 8 Press **Enter** to continue with LMS 4.2.4 upgrade.

An Application upgrade successful message appears.

Installing LMS 4.2.4 on Windows

To install LMS 4.2.4 on a Windows system:

Step 1 Log in as administrator to the system where you want to install LMS 4.2.4 and navigate to the location where you have downloaded the lms4_2_4_win_k9.zip.

Note We recommend that you run the installation from a local hard drive to avoid errors that may result from the network being slow or busy.

Step 2 Unzip the lms4_2_4_win_k9.zip file.

The contents of the zip file are extracted under the lms4_2_4_win_k9 directory.

Step 3 Double-click on the lms4_2_4_win_k9.exe file.

A warning message appears:

```
Warning: Automatic data backup does not happen during this installation. We recommend you
to take a backup of data before starting this installation.
```

Step 4 Click **Yes** to proceed or **No** to exit installation

If you choose to proceed with the installation, the Prerequisites window appears.

Step 5 Read the prerequisite details and click **OK.**

Step 6 Click **Install** in the LMS setup window.

The Installation Completed wizard appears.

The Installation Completed wizard has view buttons that allow you to view the following details:

- Errors and Warnings
- Installation Information
- Health Monitor Report

Errors and Warnings

The View button will be enabled only if errors are encountered during installation. You can view the error details on clicking the View button.

Installation Information

Provides information on how to download and install the latest Service Packs, Point Patches, Device Package updates, Config Templates, or the User Tracking Utility 2.0. If the number of managed devices exceeds 5000, only Inventory, config, and Image Management functions can remain enabled. Choose **Admin > System > Device Management Functions** to disable the other functions. However, you can set up LMS in another server to enable all the other functions for the additional devices.

Health Monitor Report

The Health Monitor report provides the following Hardware Parameter details:

- Memory availability
- Swap
- CPU
- DSN
- Backup status
- Number of MIB objects being polled
- Maximum number of MIB objects that can be managed
- Syslog database size

Step 7 Click **Finish** to exit the Installation Completed wizard.

Re-installing LMS 4.2.4

Re-installation is installing the product over the existing one without performing an uninstallation.

You can re-install LMS 4.2.4 by running the installation program on the system currently running the product.

Re-installation preserves the settings from the previous installation.

LMS applications will automatically be installed in the same location, where the previous version was installed.

Note If a file in LMS 4.2.4 is corrupted, first uninstall LMS, then install LMS 4.2 followed by LMS 4.2.2 and LMS 4.2.4.

Re-installing LMS 4.2.4 in Solaris

To reinstall LMS 4.2.4 in Solaris:

Step 1 Navigate to the location on your system, where you have downloaded the lms4_2_4_sol_k9.zip.

Step 2 Unzip the lms4_2_4_sol_k9.zip file.

The contents of the zip file are extracted under the lms4_2_4_sol_k9 directory.

Step 3 Navigate to the lms4_2_4_sol_k9 folder.

Step 4 Run the installation setup script by entering:

```
# sh setup.sh
```

or

```
# ./setup.sh
```

A Welcome message appears:

```
Welcome to Cisco Prime LAN Management Solution 4.2.4 setup program.
```

A prompt appears:

```
Press Enter to read/browse the following license agreement:
```

Step 5 Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
Do you accept all the terms of the License Agreement? (y/n) [n]:
```

Step 6 Enter **Y** to accept the license agreement and proceed with the installation, or enter **N** to deny and quit the installation.

While installing from the network drive, the Installing from Network Drive message appears.

Installation from the network drive will be slower than installing from the local drive.

Step 7 Enter **Y** to proceed or **N** to exit installation.

If you enter **Y**, then the following warning message appears:

```
WARNING: Automatic data backup does not happen during this installation. We recommend you
to take a backup of data before starting this installation.
```

Step 8 Enter **Y** to proceed or **N** to exit installation.

If you enter **Y**, then the following warning messages appear to inform you to install the Cluster Patches required for Solaris 10:

```
WARNING: Ensure that you have installed the recommended Solaris 10 cluster patches
released on Apr/17/07, in this server.

WARNING: If these cluster patches are not installed, please download and install them
from http://www.sun.com/.

WARNING: Otherwise, some features of the Cisco Prime applications will not function
properly.

Do you want to continue the installation? (y/n) [y]:
```

Step 9 Enter **Y** to proceed with the installation.

A warning message appears:

```
WARNING: Cisco Prime LAN Management Solution 4.2.4 is already installed in your system.
Do you want to reinstall?
```

Step 10 Click **Yes** to proceed or **No** to exit installation.

A list of other warning messages appears finally before the installation completes successfully.

Note LMS 4.2.4 installation automatically uses the installation mode that you selected while installing LMS 4.2.3 /LMS 4.2.2 You cannot change the LMS 4.2.4 installation mode.

Re-installing LMS 4.2.4 in Windows

To reinstall LMS 4.2.4 in Windows.

Step 1 Log in as administrator to the machine where you want to install LMS 4.2.4.

Step 2 Navigate to the location on your system, where you have downloaded the lms4_2_4_win_k9.zip.

Step 3 Unzip the lms4_2_4_win_k9.zip file.

The contents of the zip file are extracted under the lms4_2_4_win_k9 directory.

Step 4 Double-click on the lms4_2_4_win_k9.exe file.

A warning message appears:

```
WARNING: Automatic data backup does not happen during this installation. We recommend you
to take a backup of data before starting this installation.
```

Step 5 Click **Yes** to proceed or **No** to exit installation

If you click **Yes**, then the following warning message appears:

```
Warning: Cisco Prime LAN Management Solution 4.2.4 is already installed in your system.
Do you want to reinstall?
```

Step 6 Click **Yes** to proceed or **No** to exit installation.

The Prerequisites window appears.

Step 7 Read the prerequisite details and click **OK**.

Step 8 Click **Install** in the LMS setup window.

The Installation Completed wizard appears

Step 9 Click **Finish** to exit the Installation Completed wizard.

Upgrading to Cisco Prime LAN Management Solution 4.2.4

Table 1 shows the upgrade paths that are supported in LMS 4.2.4.

Table 1 Upgrading to LMS 4.2.4

Current LMS Version	Type of Upgrade	Procedure
LMS 4.2.1	Remote migration	1. Install LMS 4.2.2. 2. Install LMS 4.2.3. 3. Install LMS 4.2.4. 4. Migrate your data to LMS 4.2.4 using the instructions explained in the section Remote Upgrade to LMS 4.2.4.
	Direct migration	1. Install LMS 4.2.4 over LMS 4.2.3 or over LMS 4.2.2. The data is automatically migrated during installation.
LMS 4.2	Remote migration	1. Install LMS 4.2.2. 2. Install LMS 4.2.3. 3. Install LMS 4.2.4. 4. Migrate your data to LMS 4.2.4 using the instructions explained in the section Remote Upgrade to LMS 4.2.4.
	Direct migration	1. Install LMS 4.2.4 over LMS 4.2.3 or over LMS 4.2.2 The data is automatically migrated during installation.
LMS 4.1	Remote migration	1. Install LMS 4.2. 2. Install LMS 4.2.3. 3. Install LMS 4.2.4. 4. Migrate your data to LMS 4.2.4 using the instructions explained in the section Remote Upgrade to LMS 4.2.4.
	Direct migration	1. Install LMS 4.2. 2. Install LMS 4.2.2. 3. Install LMS 4.2.4 over LMS 4.2.3 or over LMS 4.2.2 The data is automatically migrated during installation.

Note For upgrading LMS 4.0 and LMS 4.0.1 to LMS 4.2, refer to Migrating Data to Cisco Prime LAN Management Solution 4.2 in *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*. Follow the steps in Table 1 for upgrading from LMS 4.2, LMS 4.2.2, and LMS 4.2.3 to LMS 4.2.4.

Remote Upgrade to LMS 4.2.4

To upgrade from the previous versions of LMS to LMS 4.2.4:

Step 1 Log into the machine where the previous version of LMS is installed.

Step 2 Take a backup of the LMS data.

Step 3 Log into the machine where LMS 4.2.3 or LMS 4.2.2 is installed.

Step 4 Follow the install procedure to install LMS 4.2.4. See Installing Cisco Prime LAN Management Solution 4.2.4.

Step 5 Migrate the data to LMS 4.2.4.

For Solaris:

a. Stop the daemon manager by entering:

```
/etc/init.d/dmgtd stop
```

b. Restore the backed up data by entering:

NMSROOT`/bin/perl` *NMSROOT*`/bin/restorebackup.pl -d` *BKP* [`-t` *temporary_directory]*

where *BKP* is the backup directory and NMSROOT is your Cisco Prime Installation directory.

You must give the absolute path for *BKP*. For example, if *BKP* is under /opt, give the path as *NMSROOT*`/bin/perl` *NMSROOT*`/bin/restorebackup.pl -d` */opt/BKP*.

c. Examine the restorebackup.log files

d. Start the daemon manager by entering:

```
/etc/init.d/dmgtd start
```

For Soft Appliance:

a. Stop the daemon manager by entering:

```
/etc/init.d/dmgtd stop
```

b. Restore the backed up data by entering:

NMSROOT`/bin/perl` *NMSROOT*`/bin/restorebackup.pl -d` *BKP* [`-t` *temporary_directory]*

You must give the absolute path for *BKP*. For example, if *BKP* is under /opt, give the path as *NMSROOT*`/bin/perl` *NMSROOT*`/bin/restorebackup.pl -d` */opt/BKP*.

c. Examine the restorebackup.log files

d. Start the daemon manager by entering:

```
/etc/init.d/dmgtd start
```

For Windows:

a. Stop the daemon manager by entering:

```
net stop crmdmgtd
```

b. Restore the backed up data by entering:

NMSROOT`\bin\perl` *NMSROOT*`\bin\restorebackup.pl -d` *BKP* [`-t` *temporary_directory]*

You must enter the absolute path for *BKP*. For example, if *BKP* is under C:\, enter the path as *NMSROOT*`\bin\perl` *NMSROOT*`\bin\restorebackup.pl -d` *C:\BKP*.

c. Examine the restorebackup.log files.

d. Start the daemon manager by entering:

```
net start crmdmgtd
```

For the detailed procedure of migrating and restoring the LMS data, follow the procedure in Migrating Data to Cisco Prime LAN Management Solution 4.2 in *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*.

Notes for Remote Upgrade

While setting up HA and DR environment in LMS server, ensure to set them prior to LMS installation. For further information on HA/DR configuration, see Setting Up Cisco Prime LMS in High Availability and Disaster Recovery Environment in *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*.

Bugs

This section explains:

- Using Bug Toolkit
- Open Bugs for Cisco Prime LAN Management Solution 4.2.4
- Resolved Bugs in Cisco Prime LAN Management Solution 4.2.4

Using Bug Toolkit

In CiscoWorks LMS 4.0 and later, use the Bug ToolKit to view the list of outstanding and resolved bugs in a release. This section explains how to use the Bug ToolKit through the following subsections:

- Search Bugs
- Export to Spreadsheet

Search Bugs

This section explains how to use the Bug ToolKit to search for a specific bug or to search for all the bugs in a specified release.

Step 1 Go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

You will be prompted to log into Cisco.com. After you log in, the Bug Toolkit page opens.

Step 2 Click **Launch Bug Toolkit**.

Step 3 To search for a specific bug, enter the bug ID in the **Search for Bug ID** field and click **Go** in the **Search Bugs** tab.

To search for all the bugs in a specified release, enter the following search criteria in the **Search Bugs** tab:

- Select Product Category—Select **Cloud and Systems Management**.
- Select Products—Select **CiscoWorks LAN Management Solution 4.0 and later** from the list.
- Software Version—Select **4.2.4** to view the list of outstanding and resolved bugs in Cisco Prime LAN Management Solution 4.2.4.

- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.
- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, select **Use custom settings for severity, status, and others** and provide the following information:
  - Severity—Select the severity level.
  - Status—Select **Open**, **Fixed**, or **Terminated**.

    Select **Open** to view all the open bugs. To filter the open bugs, clear the Open check box and select the appropriate sub-options that appear below the Open check box. The sub-options are New, Held, More, Open, Waiting, Assigned, Forwarded, Postponed, Submitted, and Information Required. For example, if you want to view only new bugs in Cisco Prime LAN Management Solution 4.2, select **New**.

    Select **Fixed** to view fixed bugs. To filter fixed bugs, clear the Fixed check box and select the appropriate sub-options that appear below the fixed check box. The sub-options are **Resolved** or **Verified**.

    Select **Terminated** to view terminated bugs. To filter terminated bugs, clear the Terminated check box and select the appropriate sub-options that appear below the terminated check box. The sub-options are **Closed**, **Junked**, and **Unreproducible**. Select multiple options as required.
  - Advanced—Select the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
  - Modified Date—Select this option if you want to filter bugs based on the date on which the bugs were last modified.
  - Results Displayed Per Page—Select the appropriate option from the list to restrict the number of results that appear per page.

Step 4 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Export to Spreadsheet

The Bug ToolKit provides the following options to export bugs to a spreadsheet:

- Click **Export All to Spreadsheet** link in the Search Results page under the Search Bugs tab. Specify file name and folder name to save the spreadsheet. All the bugs retrieved by the search will be exported.
- Click **Export All to Spreadsheet** link in the My Notifications tab. Specify file name and folder name to save the spreadsheet. All the saved bugs in all the groups will be exported.

If you are unable to export the spreadsheet, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Open Bugs for Cisco Prime LAN Management Solution 4.2.4

The open bugs describe possible unexpected behavior in Cisco Prime LAN Management Solution 4.2.4 release. These bugs may also be open in previous releases.

Refer to Using Bug Toolkit for querying and searching bug details.

Table 2 contains the open bugs in LMS 4.2.4.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4

Bug ID	Description
Administration	
CSCuh30757	LMS 4.2.4: Remote SSH service is affected by multiple vulnerabilities.
CSCuh54766	ActiveMQ: Allows anonymous connections from remote hosts.
CSCty29145	Serviceability items that TAC had discussed.
CSCug49234	LMS CLI access authentication via external AAA does not work.
CSCug24451	Parameter Based Redirection and Cross Site Scripting.
CSCug04143	Search and delete is deleting all devices from Inventory.
CSCue79901	Apache not starting because of presence of httpd.pid file in Linux.
CSCtz64733	Casuser to be added in "Deny"Log on through Terminal Services policy.
CSCuc03522	LMS 4.2.2: Product Feedback tab should be displayed with appropriate version.
CSCud52586	LMS 4.2.3: Exception scenarios in backup conflict notification.
CSCuh05705	Cmd svc hangs with WLC devices when wrong user name password is used.
CSCug83042	LMS 4.2 and ACS 5.x integration for Authentication needs to be documented.
CSCug69536	Security vulnerabilities in Soft Appliance.
CSCtl85879	PSB: Missed mandatory requirements in LMS 4.1.
CSCtq06652	Bulk import from RemoteNMS like HPOV and NETVIEW does not work in Soft Appliance.
CSCtx37339	Default Credential not working for cluster updated devices.
CSCty11400	NS_REF files need to be generated with FQDN instead of hostname.
CSCtz33475	Tomcat does not start if /tmp/java.cmds from previous run is not deleted.
CSCub58862	AddUserCli.pl in LMS 4.x is not working when importing users from LMS 3.2
CSCub96669	Discovery is hanging after discovering some devices.
CSCub70369	Files required for remote database access need to be shipped with LMS.
CSCuc82281	DCR Server is taking a long time to initialize.
CSCud47770	Cisco.com certificate addition.
CSCud85808	Mismatch in Integration utility versions.
CSCue03737	Apache 2.2.22 patch for RSAC images.
CSCue59593	RSH Daemon is Enabled.
CSCue31315	Cisco Prime shortcut not working after Hostname Change.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCue35742	IPPhones not getting filtered if both CDP and LLDP modules are selected.
CSCtx20910	Issue in selftest report status for HUM.
CSCtx24320	User should be notified when DFM port limit is exceeded.
CSCub85008	LMS 4.2.2: File permissions changed for upm.db on running dbunload.
CSCud56640	Unable to get debugger statements in IfAdminStatus log file.
CSCub55281	Last Updated Field for TAC case never gets updated in Support Case View.
CSCub58041	Sender Email ID is not dynamic in Support Settings configuration.
CSCua73689	SI: LMS 4.2.2: Open TAC Case tool is not opening from Troubleshooting flow.
CSCub55909	Software version is not updated during TAC case creation.
CSCuc16440	Not able to access Support Forums through Smart Services.
CSCuf52590	Occasionally active OperationallyDown events are being cleared by DFM.
CSCtr64112	ETSGJ-CH: Japanese characters are displayed in problem description while creating a TAC page.
CSCtr35154	Editing an RBAC user retains all the existing customers groups.
CSCuf77808	Defunct processes getting created in Solaris while running discovery.
CSCuj10735	"Use DCR as Seed List" option is not taking credentials from DCR.
CSCuj23645	SWIM Upgrade analysis failed for ASR1001 device.
CSCuj73450	The functionality of the collection summary portlet needs to be documented if there is a discrepancy.
CSCuj78622	LMS 4.2.4 is unable to recognize WLAN controller traps.
CSCul28294	Documentation does not support commands such as ping and so on.
CSCul38980	Null response from cmdsvc has to be handled.
CSCul54151	Display and Sort inconsistencies of dates occur in Job Browser.
CSCul95145	Displaying devices in UDG of Device Selector is taking time.
CSCum02504	Known devices are shown under "Unknown device type" group category.
Backup and Restore	
CSCuf29846	LMS backup is hard to schedule.
CSCui75731	Internal DB pointers are not properly updated during LMS 4.2.x restore backup.
Configuration	
CSCua12183	Policy Group UI stuck when the policy is clicked- New/revisit the screen.
CSCti54491	Issue in data displayed in event forensic.
CSCuh38506	LMS 4.2.4: OS type shown wrongly for ASA\ASASM device.
CSCuh51430	Archive polling hangs for URN Not found Exception.
CSCuh53609	LMS cannot archive config for FWSM with large "show context" output.
CSCty79172	LMS 5K: Job time out issue in PSIRT Collection.
CSCua12212	Profile with duplicate policy- Fix Violation "Not Attempted".

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCua12221	Fix violation fails if TFTP/SCP/RCP is the transport protocol.
CSCud61547	LMS 4.2.3: Exclude command did not exclude the entire content.
CSCti37235	LMS 4.0: User Based Role Issues in LMS.
CSCug29413	Potential to Run Arbitrary commands as root from CLI.
CSCtl21503	RBAC Issues in Template Center- Basecode.
CSCtn39216	LMS 4.0.1: RBAC Device authorization not working in Some Config Portlets.
CSCtq53879	Cache issue in OOTB Port related template on Preview CLI command.
CSCtr37756	Showing error message in UI, while deploying the PM template in switches.
CSCts52554	Port groups are not showing for Network Operator and User defined role.
CSCtt80082	Issue in OOTB, Running Config from device flow LMS4.2.
CSCtt46555	LMS 4.2: Issue with Global commands in Module based templates.
CSCtt43887	LMS 4.2: Issue with Text-area control with Template Unique Parameters.
CSCtw46829	LMS 4.2: Showing wrong job status while deploying config through TFTP.
CSCtu39092	LMS 4.2: Job Summary should change for Failed Job in config modules.
CSCtw64274	Xplatform: Config archives not restored if Custom arch location is used.
CSCtw86891	LMS 4.2: In PSIRT violation page, snmp strings are showing as clear text.
CSCtw83109	LMS 4.2: Devices are showing “Not attempt” state after completing the SIC job.
CSCtx34618	Issue in Check syslog host related parameter rule in Logging and Syslog.
CSCtx23446	LMS 4.2: Issue with Compliance Audit settings with RBAC custom user role.
CSCtx19732	LMS 4.2: No details displayed for PSIRT Jobs in Admin Job Browser.
CSCtx11146	LMS 4.2: Negative values in PSE report for Device Type Cat 4506.
CSCtx03264	LMS 4.2: Issue with the PoE and Unused PoE report data.
CSCtx26377	RBAC: Issue with Helpdesk user report generation.
CSCtx68580	OgsRMEDeviceTable not updated with new value after a config change.
CSCty65794	“Suggested Fix”,“Violation with and without fix” info popup is not generating.
CSCty61625	Preview- CLI commands are not generating if test area list is empty.
CSCtz12548	LMS 4.2.1: PSIRT SW EOL report data discrepancy.
CSCty96644	UDLD Policy 1st rule no violation.
CSCtz31077	LMS 4.2.1 Total Violations Column not sorting properly in Compliance Check Report.
CSCua11825	LMS 4.2.1: New Template Import 'Failed' in Windows and Solaris Servers.
CSCua12204	Policy violation page launch hangs for 4.2 jobs executed in 4.2.1
CSCua80090	Discrepancy between System and edited System Defined Policies (no rule change).
CSCua85435	Config Archive purging throwing Error while deleting through CWCLI.
CSCua85611	Config Archive Purge System-defined jobs are failed with timeout issue.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCub27995	LMS 4.2.2: Issues in exporting config through Remote cwcli on browser console.
CSCub90254	Error Message is displayed twice in a Pop-up when JRM is down.
CSCuc00379	LMS 4.2.2: Throwing HTTP error in Custom Queries on selecting a single device.
CSCuc06511	Daemons.log is increasing rapidly due to PSIRT Job.
CSCub78746	LMS 4.2.2: Improper text alignment in Inventory System Job schedule page.
CSCub78641	LMS 4.2.2: Issue in generating device attribute Reports.
CSCub78697	LMS 4.2.2: Issue in Inventory report generation with suspended devices.
CSCub79528	Config Archive Page: Cannot stop job in Running Status.
CSCud69642	Product family not loading in Smart Install director flow LMS 4.2.2.
CSCud77669	Config and VLAN Fetch not working through RCP on solaris server.
CSCue97433	LMS 4.2.3: VSS device is not added in DCR after conversion.
CSCuf31365	LMS 4.2.4: Changes made through netconfig are not shown for routers.
CSCug06953	Config polling and fetch results are not updated or reflected properly.
CSCuf89583	Nodes are not selected after expanding parent - Baseline compliance.
CSCug60308	Mismatch in overall count under Config Archival Summary page.
CSCue36113	LMS generates SSH security errors while connecting to IOS-XR device.
CSCuh44152	Crmtftp server does not allow copy operation without an empty file.
CSCua16488	LMS 4.2.1: TrustSec: SXP, SGA template deploy job is running for a long time.
CSCtu41186	SNMP config on 6k via LMS is not working correctly.
CSCub35950	Role Based Access is not available for Smart Interaction.
CSCub34961	Support Case information is not retained during LMS flows navigation.
CSCtq96670	Issues in SI Configure Flow.
CSCtu29727	LMS 4.2: Unhandled SSHV2 Message should be provided as generic message.
CSCtu21015	LMS 4.2: Module device is not able to fetch ShComplnceReportCmndset.
CSCuh59421	LMS 4.2.4: Issue in "IOS Software IPS DoS Vulnerability-20120926" validation.
CSCuh59444	LMS 4.2.4: Vulnerable image check is not proper.
CSCui04360	Single device export in CSV format for DDR is not working in IE.
CSCui59990	Log rotation job archives the content with empty space when original log file is in use.
CSCuj12692	LMS 4.2 - Non Cisco device is recognized as Cisco Call Manager.
CSCuj30568	The cwcli command does not work when there are special characters in credentials.
CSCuj47117	Archive poller exhibits job hung issue inconsistently.
CSCuj60875	LMS 4.2.4: SWIM support is required for Nexus 1000V.
CSCuj61704	There is no support for 3850-24p-L in LMS 4.2.3.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCuj85194	LMS 4.2: The user-defined description is not available in the detailed device report for Nexus devices.
CSCul19863	Config Fetch failed with DeviceContext error.
CSCul38962	Syslog dropping issue needs to be avoided.
CSCul56156	LMS 3.2(1): Information is missing in the compliance template table when using IE8.
CSCum29217	Baseline template issue occurs with submode command during compliance check.
CSCum48224	Error message is displayed when generating All Host Entries report in active status.
CSCum53711	Unable to view Config and endhost report while accessing Troubleshooting workflow using IP address.
CSCum60067	Nexus 5k Devices consume more memory space during inventory job.
Dashboard and Portlets	
CSCua91495	UII Dashboard is sending GET request in case of large number of records.
CSCug71773	LMS 4.2.2 Invalid LMS Server link.
CSCto77270	Issue in Hum portlets.
CSCtw76726	LMS 4.2: Undeployed portlet in 32SP public dashboard from 32sp migration.
CSCto52631	Issue in time display of EW ST and PC graph portlet.
CSCto85894	Issues in NAM Portlets.
CSCue19794	CiscoWorks Portal menu is not available in Debug Settings.
CSCue19666	“About” page shows 4.1 in RSAC server.
CSCtn77403	LMS 4.1: Friendly URL is not getting updated with Parent Dashboard for Child.
CSCtw57814	Template changes are not getting reflected in poller.
CSCtw63795	Issue in Exclude and Include options in Pollby pattern preference.
CSCtq29576	Issue in instance name for mem util template.
CSCui60769	UT collection summary portlet shows ANIDBEngine down when DB engine is up.
Discovery, Device Management, and Grouping Services	
CSCtw57078	Inventory Hardware report shows mismatch in the columns.
CSCts30685	Wrong energywise details are displayed in inventory change details.
CSCtt02540	LMS 4.2: Summary verification of Custom inventory have mismatch of details including templates rules with details entered in column.
CSCtv10861	LMS 4.2: Issue with combination of new and old attribute in Inv Custom.
CSCtv11780	LMS 4.2: Failed to generate report System: Management Type attribute.
CSCtu26759	LMS 4.2: Report generation failed in some scenarios in inv custom template.
CSCuf16312	In Inventory Collection Job Details, device sort is not working.
CSCug56285	LMS 4.2.4: Inventory polling failed when v2c alone is enabled.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCub57989	Cat4500X - CM Auto Support - Duplication appears in Device Attributes Report.
CSCtx50661	Unable to stop the running discovery instance error message in discovery.
CSCty01415	ETSGJ-CH: LMS Fault monitor links appearing in CS Edit device identity.
CSCty15348	Patch for the defect CSCtr77570 needs a repost.
CSCub20363	Largest Free Buffer value shows "UNKNOWN".
CSCuh03125	Acquisition Action: wrong type of devices displayed in the error message.
CSCuc78315	LMS 4.2.2: IP is not getting updated for endhosts in dynamic UT.
CSCtz12120	LMS 5K: No Data available is shown as Device Details during loading time.
CSCts91474	LMS 4.2: Information is missing while creating PDF format of Inventory custom report.
CSCtx23609	ETSGJ-CH: Error popup is thrown when launching config archive summary page.
CSCtu29863	Report failing in EM when cross launched from FM.
CSCti40318	RBAC: Issues with IPSLA and Hum Task.
CSCtg43837	Able to perform any operations with collectors of unauthorized devices.
CSCtx44101	ETSGJ-CH: Device Status Failure variables page is showing error.
CSCtx44121	ETSGJ-CH: Print View is truncated for all reports.
CSCti70459	M&T RBAC-Issue in custom role with user defined task.
CSCtw52350	LMS 4.2: Fault Customizable groups are lost after editing as private.
CSCtq61855	Issues in Report Jobs problem in IPSLA.
CSCtw81614	Device type is unknown in DFM when device is managed from suspended.
CSCuf94029	LMS System log status reporting 0 byte files as an exception.
CSCud26805	LMS 4.2.2: Patch: Not able to create TAC service request for Catalyst 6503.
CSCuh86945	EOL/EOS Hardware report showing incorrect number of modules.
CSCui02359	LMS 4.2 - Group Selector option does not work with User Defined Groups.
CSCui14011	LMS displays VTP version 4 when VTP version 3 is used.
CSCui76798	Inventory Detailed Device report is not displayed in IE 8.0 when running an Immediate job report.
CSCui87081	Customer Inventory report includes "Interface:Last Change:=:All" as future dates.
CSCui87252	Customer Inventory report with "System:SysUpTime" reports incorrect System Up Time.
CSCui91147	SNMPv3 managed devices are incorrectly exported by Export Data for PI.
CSCui14512	HTTP Status 500 error is thrown when live graph/ histograph is launched for a device.
CSCuj23988	Serial number of FWSM module is missing in the Inventory Report.
CSCuj29317	LMS 4.2.4 - Inventory Collection fails for ONS15540 device.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCuj34851	LMS 4.2.x: Importing device groups from an XML file may partially fail.
CSCuj49204	False prefixLength messages of type "New" are displayed in the inventory change report.
CSCul15180	Event Forensics connections to devices are not released.
CSCul19902	The VSS device details are not collected by data collection and user tracking.
CSCul24801	Export and SSH are not working on LMS 4.2.4.
CSCum34954	Inventory detailed report for ASA 5510 device does not contain memory information.
Installation	
CSCts55260	CARS CLi command execution issues.
CSCtr66880	Soft Appliance installation mandating the Name server input.
CSCtr22450	Linux CARS CLI option "Reset-config" doesn't work for LMS.
CSCtr28929	Issues while executing CARS CLI commands.
CSCuc80880	OS Syslog should be disabled by default.
CSCtz28984	LMS 4.2.1: Issue with the 4k device families removal in metadata and TrustSec.
CSCtz86097	LMS 4.2.1: TrustSec Readiness, Issue with the Cat6k devices filtered.
CSCua16467	LMS 4.2.1: EnergyWise Issue with Multicast Environment.
CSCuc18150	EnergyWise does not detect endpoint moving to a different switch port.
CSCui00717	LMS EnergyWise endpoints not added to group if the Role is defined as "AIR-CAP*".
Monitoring and Troubleshooting	
CSCuc06771	Self-Test shows as FAIL for swap size.
CSCug97521	LMS 4.2.4: Filter option is not working properly in Fault monitor page.
CSCug77061	Reachability status shows failed when managed with Host name.
CSCtx34369	Trustsec status values to be changed accordingly in technolgy details.
CSCuc70650	Inventory Data is not available in Trouble shooting page for SG device.
CSCub74971	Invalid Email address is accepted by address field in Fault Email Notification.
CSCud48057	LMS 4.2.3: Syslog AA Validation on adding and deleting a user from Group.
Network Topology, Layer 2 Services, and User Tracking	
CSCuh38258	Need to Document IPM supported and Unsupported devices.
CSCuf06338	LMS 4.2.4: Page Alignment Issue on Data Metrics report page
CSCti22737	Issue in Event forensic data with subinterfaces.
CSCud48575	Cisco 1130 Access Point not supported in LMS 4.0 User Tracking.
CSCue99483	UT Acquisition hangs due to IOException.
CSCth60000	Alerts are to be cleared from Topology after DFM Functionality disable.
CSCtx11751	Issue in Dual IPV6 Configuration device.

Table 2 Open Bugs in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCug01434	LMS 4.2.4: Ipv6 address report is not launching for latest IOS images.
CSCtr01442	LMS 4.1: Timeout issue in CMDSVC in Catalyst 4500 Platform Configuration.
CSCug29234	RSAC syslog daemon dropping syslogs.
CSCsv97508	SNMP Call to a particular device hangs.
CSCui24841	Issue in stack member support for Cisco 3750 Stack devices.
CSCui44610	Topology endhost is not shown in device center.
CSCui55114	LMS 4.2.x Compliance report capability issue for Nexus devices.
CSCui56419	Ethernet Bus Links position layout is not saved in Layer2View.
CSCui66527	Switch port traffic disruption occurs when Config Editor deploy changes to allowed vlans.
CSCui70500	LMS 4.2.3 - Stale historical link details from topology services.
CSCui75606	Crmlog service performs DNS queries even if CrmDnsResolution is set to 0.
CSCui76739	PI 1.3.1 CA is not closing up the SSH Session with N7k and N5k devices.
CSCui94700	LMS 4.2 - Nexus 7K running 6.1 cannot be managed due to Inventory Collection failure.
CSCuj99377	Some duplicate MAC addresses are missing in the end host report.
CSCul25152	LMS-The Trustsec dashboard is not working.
CSCul97455	Acknowledged discrepancies appear as 'not acknowledged' after LMS restart.
CSCum41633	LMS 4.2.x Compliance report capability issue for Cisco Catalyst 6500 Series Firewall Services Module.
CSCum53665	LMS 4.2.4 cannot import s72033-ipbase-mz.151-2.SY1.bin images.
CSCum58402	Cat4507R+E devices do not show any IOS-XE images while downloading images from Cisco.com to SWIM repository.
UII	
CSCub82240	Status is not shown for the Variables - FMDevUpd v3.0 LMS 4.2.1.
CSCtl44985	Unable to configure IPv6 devices in the ASP Interface Configuration page.
CSCto04284	LMS 4.1: Manage ASP flow- wrong display of Macro Name.
CSCty76737	The BRI Ports are not being updated in LMS.
CSCtn68202	Issue in hum when entPhysicalDescr names are same for different instances.
CSCtr32047	ETSGJ-CH: Collector Export to a Japanese Text file fails.
CSCua52798	NGA - Version is not displayed in the UI of Device Attributes LMS 4.2.
CSCua73478	Processing status message needs to be changed.
CSCuc49806	LMS 4.2.2: Choose file button is not working in Support case window.
CSCui12233	LMS 4.2.4_1.5K: GUI is not launching in Linux Endurance Server.
CSCui26933	User Defined Device Group import fails if group is already defined.
CSCui57434	Version change is not reflected after upgrading LMS 4.2.3 to 4.2.4.

Resolved Bugs in Cisco Prime LAN Management Solution 4.2.4

Table 3 contains the bugs resolved in LMS 4.2.4.

Refer to Using Bug Toolkit for querying and searching bug details.

Table 3 Bugs Resolved in Cisco Prime LMS 4.2.4

Bug ID	Description
Administration	
CSCuc79454	mem.pl incorrectly shows RAM and SWAP as fail in Virtual Appliance.
CSCuc91527	LMS is susceptible to DOS attack.
CSCuc93380	LMS 4.2.3: Error popup is not thrown on updating SWIM synchronization job.
CSCue06188	LMS 4.2.3 bug fix CSCub77461 is breaking RME Device Selectors functionality.
CSCue06195	Running dbrestoreorig.pl on CMF is making DCRServer not to start.
CSCue15844	LMS 4.2.3_1.5K: Hprof files are created for some processes in endurance server.
CSCue32038	Discovery Seed Device Settings is accepting regex, but not working.
CSCue38901	Discovery adds devices with IP address even though DNS is working.
CSCue46973	SelfTest wrongly reporting SWAP Space failed for 400 devices license.
CSCug30673	JRE and JPI upgrade.
CSCug45595	FireFox 19.0 version support for LMS.
CSCug51521	Contract Connection reports not working.
CSCug56346	LMS 4.2.4: Sorting is not working in Process Management page.
CSCug77823	Cross Frame Scripting vulnerability in LMS.
CSCug84730	NCS: Export complete data taking more time in Endurance server.
CSCug97439	LMS 4.2.4: Compliance purge option is not working in migration servers.
CSCuh36203	LMS 4.2.4: SWAP validation was done incorrectly for license 1000 to 1500.
CSCuf25313	Help Tag needs to be added in cwhp-sitemp.xml file for User Accounts Setup page.
CSCsc41885	Rediscovery Schedule warning message should be changed.
CSCub78795	LMS 4.2.2: Issue in Fault Notification group page.
CSCue19782	Authentication Mode changes are not printed in the log file.
CSCue44971	Cisco.com credential validation URL needs to be changed.
CSCug48797	Need support for Firefox 19 and ERS17 version.
Backup and Restore	
CSCub47690	Fault and job information are to be extracted from extracting ExportOnly.zip folder.
CSCuc25306	Swim_Change_History_871.csv file is displayed under backup\settings\MIBS folder.

Table 3 Bugs Resolved in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCud66192	LMS 4.2.3: Custom path SWIM,Archive data is missing in exported backup directories.
CSCue01860	NCS 2.0: Checksum issue is generated while migrating LMS Data to External Server.
CSCuf36680	Devices exported from LMS 4.2.4 not imported in PI2.0.
CSCug07252	Unable to schedule a backup due to conflicting jobs.
CSCuh27285	Backup version to be supported from LMS 4.2.2 onwards in LMS 4.2.4.
CSCug10661	LMS 4.2.4 Migration Support need to be tracked.
Network Topology, Layer 2 Services, and User Tracking	
CSCtz91163	ISR routers not showing links in topology between serial interfaces.
CSCud89429	Switch port report showing duplicate entries/wrong data.
CSCue18533	Data collection run every 10 mins for unsupported device.
CSCue84284	Data collection is not collecting/updating device details.
CSCue84329	Data collection is hanged, because of port channel name NULL value.
CSCug16053	Data collection Collection Scheduler should run based on property.
CSCug84821	End_Hosts ani view is not having firstSeen details.
CSCts36544	Endhost hostnames may be incorrect.
CSCuf30388	LMS 4.2.4: Cmapps.log is not getting updated in Windows.
CSCuf66330	User tracking is not updating last seen value for end host.
CSCuf98857	LMS 4.2.4: Downloading UTU steps need to be changed as current changes.
CSCug16141	portsData.xml should have ports without VLAN mapping based on property.
CSCug27089	All Host Entries report's schedule job with "connected" status is failed.
CSCug79530	User tracking Dot1xEnabled collection should run based on property value.
CSCuh30582	Endhost's state change from inactive to active should not update endhost’s firstseen Value.
CSCuh30713	User tracking is not collecting endhost for IP configure in management interface.
CSCuf60082	Change in Portchannel status is not monitored properly.
CSCud94611	LMS 4.2.3: Periodic 'device attributes' reports are not being generated.
Dashboard and Portlets	
CSCue97545	(icn1) Remote integration data extraction issue with LMS 4.2.
CSCug39560	Exception while processing ports of C5k, C3k, c3900, c4k and c6k.
CSCuh24860	Unable to view multiple discrepancy dashboard using remote portlet.
CSCue56320	URL's on Device Request page are incorrect or broken.
CSCue57239	LMS 4.2.3 Collection Summary portlet may hang processes.
CSCtn76703	LMS 5k: VRF Collection shows running in Collection Summary portlet.
Discovery, Device Management, and Grouping Services	

Table 3 Bugs Resolved in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCtt34316	LMS 4.2: Report generated is not satisfying the rules in inv custom temp.
CSCtz70975	PSIRT report fails for CAT6k platform.
CSCua75698	HUM report showing all instances instead of applicable ports.
CSCua97512	LMS 4.2: 'Unidentified Trap' Alerts need to be more meaningful.
CSCud15801	Version change inconsistent for managed device when running inventory collection.
CSCud96552	LMS 4.2.3: Error Popup shows up in Inventory Job Browser.
CSCue05486	Exclude DFM.log and DFM1.log from DFM backup file list.
CSCue20461	Inventory Collection Hangs inconsistently.
CSCue50835	Inventory Change Report shows unreadable IFEntry ID.
CSCuf79864	Custom Inv Report is not showing module info when slotNum is null.
CSCug26725	Need provision to load MIBs in DFM on demand.
CSCug29043	LMS 4.2.3: Cannot update Inventory Config And Image Management packages.
CSCug42752	Device bulk import failed to NCS2.0(N34).
CSCug71804	Pdf file for Syslog Custom Summary report is not get attached to email.
CSCug89830	CSV file is not generated in Local Publish Path in Inventory Report Designer.
CSCue59366	ICMPJitter collector moved to Config Failed state.
CSCue84101	LMS 5K: CPU Utilization poller with less devices with instance polling state.
CSCuf15525	Config Archive jobs are not getting triggered in N28 build.
CSCug83586	Devices with no syslog report issue.
CSCug28679	ASP configuration shows first device IP while clicking preview CLI.
Installation	
CSCug99309	LMS 4.2.4: ESS Process and its related process are not up after installation.
Configuration	
CSCts48330	Heap Space is not sufficient for CWCLI command.
CSCuc67797	Histo-Graphs are in settings mode in LMS 4.x.
CSCud48443	Issue in sync archive while processing queue of device request thread.
CSCud60439	Popup is thrown with NULL statement in config page.
CSCud98952	LMS 4.2.3: ChangeAudit object may be null during VLAN collection
CSCue16791	VLAN record should be excluded in Config summary and Collection Portlet.
CSCue26786	LMS 4.2.3: UI issue in IE8 browser.
CSCue33099	UDF label's not getting reflected in RME workflows.
CSCue46025	Potential to Gain Shell with Root Privileges.
CSCue57265	LMS Configuration Archive may leave SSH sessions open.
CSCue89901	PSIRT Report fails for cat 6k device.
CSCue94863	Config archive fails due to issue in accessing vlan fetch protocol.

Table 3 Bugs Resolved in Cisco Prime LMS 4.2.4 (continued)

Bug ID	Description
CSCuf20420	Sync Archive job email attachment not enabled.
CSCuf24986	SmartInstall Configuration generating invalid commands in IE.
CSCuf46159	LMS 4.2.3 internal link not working.
CSCuf83795	LMS 4.2.3: Out of sync job is not working.
CSCuf88477	LMS Cfg Deploy fails for radius server syntax.
CSCug69267	LMS 4.2.3_1.5K: EssentialsDM process alone went down in Win1.5K server.
CSCug70949	Blank -Xmx entry is there in start_compliance_process.sh in SOL and LNX platforms.
CSCug73468	Version Summary page is small.
CSCug78909	LMS 4.2.3: Software Report taking hours to display the data.
CSCuh35076	LMS 4.2.4: CAAMServer went down in Windows.
CSCuh37673	Revert the fix CSCud48443.
CSCuh52171	LMS 4.2.4: Archive job failed after running sync archive job for a device.
CSCtz93148	Vulnerabilities reported in PSIRT ports.
CSCuc92806	LMS 5K: CAAMServer went down in our Linux 1.5K server.
CSCuf45560	LMS 4.2.4: Purge option should be provided for Compliance command collection.
CSCuf45737	LMS 4.2.4: Compliance cmd collection schedule to be changed to weekly.
CSCuh09502	LMS 4.2.4: None of the PSIRT new policies are listed in Windows.
CSCuh29589	LMS 4.2.4: Http status 404 is thrown for PSIRT report.
CSCuh36089	LMS 4.2.4: Schedule is not getting updated in Compliance data collection job.
CSCtx78019	LMS 4.1: Config Menu items are missing for non-admin user.
CSCuc76105	NCS 1.2 CA is not cleaning up the CLI Session with WLC.
CSCub00639	RME job's notification email uses incorrect format for its sent date.
CSCue05816	Need an option to disable/enable unidentified traps in dfm.
Monitoring and Troubleshooting	
CSCue28367	Exclude voice interfaces for ISR and ASR devices from DFM discovery.
CSCue52643	Device hostname issue in IPM.
UII	
CSCue59646	LMS 4.x Device update from GUI creates incorrect xml file.
CSCue37921	Common services related to web services are not running.
CSCuh16860	After stopping and starting FM the status shows indeterminate.

Product Documentation

Table 4 describes the product documentation that is available.

Table 4 Product Documentation

Document Title	Available Formats
Release Notes for Cisco Prime LAN Management Solution 4.2.4 (this document)	On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2.4/release/notes/lms4_2_4_release_notes.html
Context-sensitive online help	Select an option from the navigation tree, then click Help.

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Related Documentation

Table 5 describes the additional documentation that is available.

Table 5 Related Documentation

Document Title	Available Formats
Release Notes for Cisco Prime LAN Management Solution 4.2.3	On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2.3/release/notes/lms4_2_3_release_notes.html
Release Notes for Cisco Prime LAN Management Solution 4.2.2	On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2.2/release/notes/lms4_2_2_release_notes.html
Readme for Cisco Prime LAN Management Solution 4.2.1	On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2.1/readme/readme.html
Installing and Migrating to Cisco Prime LAN Management Solution 4.2	On Cisco.com at Installing and Migrating to Cisco Prime LAN Management Solution 4.2
Release Notes for Cisco Prime LAN Management Solution 4.2	On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2/release/notes/lms42rel.html
LMS 4.2 User Guides	On Cisco.com at http://www.cisco.com/en/US/products/ps11200/products_user_guide_list.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Release Notes for Cisco Prime LAN Management Solution 4.2.4