FLEXERA SOFTWARE

FLEXERA SOFTWARE™
FlexNet Publisher®

FlexNet Publisher 2014 (11.12.1.5) Service Pack 5
Release Notes

October-2014

Overview 2

Resolved Issues in FlexNet Publisher (11.12.1.5) Service Pack 5 2

- General Issues 2
- Dongle Issue 2

Resolved Issues from FlexNet Publisher (11.12.1.4) Service Pack 4 3

- General Issues 3
- Dongle Issue 4

Dongle Driver updates 5

Resolved Issues from FlexNet Publisher (11.12.1.2) Service Pack 2 5

- General Issues 6
- lmadmin Issues 7
- Dongle Issue 8

Resolved Issues from FlexNet Publisher (11.12.1.1) Service Pack 1 8

- General Issues 8
- Dongle issues 10

Known Issues in FlexNet Publisher (11.12.1.5) Service Pack 5 11

Supported Platforms 11

Overview

This service pack is intended to correct only the problems that are described in the release notes and only applies to the supported platforms indicated below.

Resolved Issues in FlexNet Publisher (11.12.1.5) Service Pack 5

General Issues

Linux client cumulative memory leak

Previously, Linux client applications would experience a small but cumulative memory leak with every checkout. This has now been resolved. (FNP-10226)

UMN2 not generated on Windows Server 2003

From 11.12.1.0, UMN2 was no longer generated on Windows Server 2003. This was due to the move to WMI for extracting system properties in Windows trusted storage components from 11.12.1.0 onwards. A WMI property (Physical Adaptor) was used for determining a suitable NIC candidate for UMN2. This property is not supported on Windows Server 2003. The use of WMI has now been refactored so that UMN2 is generated on Windows Server 2003. (FNP-10143)

Codesign was unable to sign libFNP shared objects produced by the preptool on OSX

FlexNet Publisher's activation library is generated as an output of preptool. This shared object is named as <PublisherName>_libFNP.dylib. Previously libFNP.dylib would fail an attempt at code signing with an "`object file format unrecognized, invalid, or unsuitable`"error. This was due to preptool processing improperly handling the `LC_DATA_IN_CODE` load command. This issue has now been resolved for empty `LC_DATA_IN_CODE` load commands. (FNP-10155)

Note • *If a populated* `LC_DATA_IN_CODE` *load command is detected, preptool terminates with an error message.*

Dongle Issue

Dongle debug information

From 11.12.1.0, `lmhostid -flexid` could emit new debug messages to stdout, even if a dongle's ID was successfully extracted. Now, the debug messages occur only with the new `lmhostid -flexid -long` command. (FNP-10223)

Resolved Issues from FlexNet Publisher (11.12.1.4) Service Pack 4

General Issues

Heartbeart connection failure when an expired borrowed license exists in the borrow cache

Previously, if a borrowed license expires in the borrow cache of a client that is imminently due to perform an automatic heartbeat to a license server, then the client may inappropriately experience a heartbeat connection timeout and exit. This has now been resolved. (FNP-9888)

Trusted storage partially vulnerable to the restore exploit

The trusted storage restore exploit is as follows:

1. activate a license to trusted storage.
2. back up trusted storage.
3. return the license to the back office.
4. restore the backed-up trusted storage, regaining the license.

FlexNet Publisher defends against the restore exploit by causing trusted storage to become untrusted in the last step above, by means of a RESTORE (anchoring) break.

Previously, due to an error in the calculation of the anchor sequence number, a restore exploit could successfully be executed some of the time. This is now resolved.

This issue was initially reported as the Win64 (x64_n6) FNP toolkit being more vulnerable to restore exploits than the Win32 (i86_n3) toolkit. However, both toolkits were affected by this issue. (FNP-9954)

UMN3 cannot be extracted on RHEL7

This affects trusted storage users activating licenses rights in RHEL7 guests. Additional methods for extracting the VMID value used in UMN3 have been added to cater for Linux installations wherein the HAL subsystem is not enabled (such as is the case with a default RHEL7 installation). Some of these methods require root privilege. In 11.12.1.4 such privilege is obtained by means of the Linux FlexNet Licensing Service, as installed by install_fnp.sh.

It is therefore now a best-practice recommendation that trusted storage servers and clients on Linux systems install the Linux FlexNet Licensing Service. (FNP-9945)

VM_UUID memory leak

Previously, using the VM_UUID license keyword (either on the SERVER line or in the lc_hostid API) would result in a small but incremental memory leak. This leak has now been removed. (FNP-9943)

Issue with lc_next_ conf API is now resolved

Previously lc_next_conf API returned only one configuration value for a feature that had multiple increment lines, now after the fix lc_next_conf returns all the configurations of the feature being used. This issue was specific to AIX. (FNP-10015)

Using WMIC to start the lmgrd-based license server

A change made in the communication protocol between lmgrd and the vendor daemon in 11.12.1.0 (to harden the license server against DoS attacks) resulted in the Windows wmic utility being prevented from starting the license server - wmic was not able to parse the command line passed from the lmgrd to the vendor daemon. This has now been resolved. (FNP-10020)

Duplicate symbol warnings in lmgr.lib

A number of duplicate symbol warnings related to linking against lmgr.lib have been removed. Some remaining duplicate symbol warnings may be observed when linking against lmgr.lib. These warnings are issued from modules with names beginning `gvm_` and also the module `GenericVMIF`; such warnings may be safely ignored.

When building an aggregate object file from the release kit library contents, modules with names matching the following patterns should be omitted:

```
*VM.o, gvm_*.o, GenericVMIF.o, VirtInterface.o
```

On Windows the filename extension will be `.obj`, not `.o` (FNP-10059)

Dongle Issue

FLEXID9 driver upgrade

FLEXID can be extracted with v6.63 on Windows 8.1, whereas v6.62 (as packaged with 11.12.1.2) did not successfully extract FLEXID9 on Windows 8.1. (FNP-9863)

Dongle Driver updates

The FLEXID 9 dongle driver updates for this service pack are summarized in the following table:

Table 1 • The version update between releases

Platforms	11.12.1.0	11.12.1.2	11.12.1.4	DLL or Shared objects packaged from 11.12.1.1
Windows	FLEXID9_Windows_v6_60_i686.zip and FLEXID9_Windows_v6_60_x64.zip	FLEXID9_Windows_v6_62_i686.zip and FLEXID9_Windows_v6_62_x64.zip	FLEXID9_Windows_v6_63_i686.zip and FLEXID9_Windows_v6_63_x64.zip	haspsrm_win32.dll version 7.1 haspsrm_win64.dll version7.1
Linux	aksusbd-redhatsuse-2.2.1.tar.gz	aksusbd-redhatsuse-2.4.1.tar.gz	aksusbd-redhatsuse-2.4.1.tar.gz	libhasp_linux_i686.so version 7.1 libhasp_linux_x86_64.so version 7.1
MAC	FLEXID9_OSX_V6.60.dmg	FLEXID9_OSX_V6.62.dmg	FLEXID9_OSX_V6.62.dmg	hasp_darwin.dylib version 7.1

Note • *The shared objects which were v7.0 on 11.12.1.0 are now v7.1 from 11.12.1.1*

Resolved Issues from FlexNet Publisher (11.12.1.2) Service Pack 2

This release of the FlexNet Publisher Licensing Toolkit resolves the following issues. (Numbers in parentheses indicate the Flexera Software issue reference number.)

General Issues

lmhostid instability in the presence of multiple ethernet adapters

Previously, in the presence of several ethernet adapters, lmhostid and the callers of the lc_hostid API may experience a segmentation fault on OS X. This is now resolved. (FNP-9885)

Upgrade of OpenSSL version 1.0.1h for Security Vulnerability in FlexNet Publisher

Flexnet Publisher now uses static versions of the OpenSSL libraries that are not impacted by the HeartBleed bug. This has been achieved by upgrading to OpenSSL version 1.0.1h which does not have this security vulnerability. (FNP-9832)

Version Compatibility

The FlexNet Publisher support statement is: version (vendor daemon) >= version (client). Previously, the license sever did not verify the version of FlexNet Publisher client during checkout process, when the client version was greater than the server version. This could result in misleading errors, making it difficult to determine that the root cause was that the vendor daemon had not been upgraded.

Now, when a checkout request is sent by a client that has FlexNet Publisher version greater than vendor daemon then error -83 (LM_SERVOLDVER) will be returned.

Current limitations of when LM_SERVOLDVER is returned are:

1. License server version >= 11.12.1.2
2. Only the first two version fields of client and server (Major and Minor) are compared.
3. This check only occurs during processing of the lc_checkout call.

(FNP-9773)

Increased connections in lmgrd

In prior releases, Windows lmgrd does not respond to FlexNet utilities or clients when more than 62 simultaneous connections were established. To increase the number of simultaneous connections, the file descriptor limit in lmgrd is increased to 1K for Windows only (FNP-9384)

Update to EXCLUDE option

Previously, additional IP addresses were getting blocked or excluded when the EXCLUDE option was used in the options file, this issue has now been resolved. (FNP-9894)

License server memory issue

Previously, a cumulative memory leak on license server may occur in the Vendor Daemon after each checkout request from a client. This issue is now resolved. (FNP-9805 and FNP-5728)

lmadmin Issues

lmadmin port selection enhancements

In 11.12.1.0 a number of lmadmin port selection enhancements were delivered, which were designed to help license administrators identify port selection conflicts. However, one unintended consequence was that when a license administrator selected a port that was already in use by lmadmin a port conflict warning message appeared, which caused unnecessary confusion. Now, port conflict warning messages will no longer appear when a port is selected that is already in use by lmadmin. (FNP-9436)

Security vulnerability issue has been addressed

The following security vulnerability problem reported for `lmadmin.exe` by Microsoft Attack Surface Analyzer has been fixed.

```
The service lmadmin is vulnerable to tampering by multiple non-administrator
accounts.
```

Details:

```
Service: lmadmin

Binary path: C:\Program Files (x86)\FlexNet Publisher License Server
Manager\lmadmin.exe

Binary path writable by:

File: C:\Program Files (x86)\FlexNet Publisher License Server Manager\lmadmin.exe

Account Rights

Builtin Users (S-1-5-32-545) FILE_WRITE_ATTRIBUTES FILE_WRITE_EA
FILE_APPEND_DATA FILE_WRITE_DATA
```

(FNP- 9764)

lmadmin GUI Concurrent tab updates

In 11.12.1.0 a new feature was introduced, after updating trusted storage hybrid licenses, an automatic reread happens based on `ls_ts_update_poll_interval` value. Previously, even after Automatic reread, the newly added features were not reflected on the concurrent tab. Now as soon as the `Automatic Reread is successful,` the concurrent tab displays the newly added features. (FNP-9694)

Note • `hasp_rt.exe` *is now packaged with lmadmin. For more information refer to the driverless dongles discussion.*

Dongle Issue

FLEXID9 dongle connection to Linux system

Previously, a vendor daemon using a FLEXID9 hostid would, after a period of time of the order of several hours to days, lose contact with the dongle and then shut down when its periodic hostid check failed. This issue has been addressed. (FNP-9698 and FNP-9757)

Resolved Issues from FlexNet Publisher (11.12.1.1) Service Pack 1

This release of the FlexNet Publisher Licensing Toolkit resolves the following issues. (Numbers in parentheses indicate the Flexera Software issue reference number.)

General Issues

Crash occurs when running activation utilities when WMI is disabled.

If WMI is disabled, the activation utilities and APIs, for example appactutil -unique, can crash. In all such cases, an appropriate error path is now followed. Publishers who run windows services which interact with FNP trusted storage components are advised to create, at install time, a dependency from their service on: FNPLicensingService or FNPLicensingService64; and the WMI "winmgmt" service. (IOA-000125134)

Unable to checkout a feature from a fulfillment record in trusted storage

In v11.12.1.0, if client trusted storage has more than one fulfillment record, and each fulfillment record has a different serverHostID, then attempting to checkout a feature can result in a `LM_BADCODE` error, when attribute *LM_A_CHECK_LOCAL_TS_SIGNATURE* is set to 1. This issue has been resolved. (IOC-000090943)

Checkout delay due to timeout issue with Amazon EC2 detection mechanism

Previously, a `lmhostid` or `appactutil` command or first call to *lc_checkout* on Linux or Windows could result in a delay of the order of minutes before the utility or API returned. FlexNet Publisher performs virtualization and cloud detection techniques during initialization. Amazon EC2 detection occurs by querying a meta-data url published by Amazon. In some networks, the IP address of this published URL may inappropriately be present, and an attempt to read from it would block. Now, FlexNet Publisher's virtualization component times out appropriately in such cases. (IOA-000124003)

OS X clients operating in complex network configurations may experience delayed checkouts

As part of the checkout operation, FlexNet Publisher performs hostname resolution by means of standard `getaddrinfo` calls. OS X machines in overly complex network configurations may experience delays in hostname resolution of the order of seconds. An example of when this can occur is when several domains are specified on the OS X client machine. This delay accumulates in the checkout call. While it is inadvisable to operate networks of this complexity, publishers cannot easily influence the network administration of their customers. Therefore, in this service pack, FlexNet Publisher's hostname resolution has been optimized. However, if checkout delays are still experienced, the new environment variable *`FNP_IP_ENV`* can be set to 1. This will bypass all hostname resolution during the checkout call, eliminating checkout delays in complex network configurations. The consequence of bypassing hostname resolution at checkout time is that IPv4 node-locked hostids cannot be supported. In such cases the hostname can be used instead of the IPv4 hostid.

Note • *OS X machines that use ".local" in the domain search path may still experience checkout delays in poorly configured networks, even when FNP_IP_ENV is set to 1. Producers who continue to experience these delays can request the IPv4 11.12.1.2 OS X kit.*

(IOC-000090921)

VM_UUID was not getting extracted from RHEL7 guests

Earlier Linux RHEL7 guests were not supported in extraction of VM_UUID (lmhostid –ptype VM_UUID).This issue is resolved. (IOB-000063682)

New lmnewlog option for secondary server

Prior to FlexNet Publisher 11.12.1.1, you could not rotate report logs with lmnewlog option on the secondary server of a triad. A new lmnewlog option "`secondary`" is introduced to serve the secondary server.

Syntax

```
lmnewlog -c triad.lic new_report_log.rl -secondary
```

Requirements:

1.Upgrade Vendor daemon to FNP 11.12.1.1.

2.Upgrade lmnewlog (lmutil) to FNP 11.12.1.1. (IOC-000090597)

Note • *lmnewlog will rotate report log on Master server when –secondary option is not used with triad servers.*

Dongle issues

FLEXID9 support safenet driverless dongles

In this service pack, FlexNet Publisher is for the first time providing experimental FLEXID9 support for SafeNet driverless dongles. Specifically, experimental support is provided for SafeNet PRO DL dongles (purple color) without drivers. Publishers wishing to test this functionality should be aware of the following restrictions

1. Although drivers are not required, the SafeNet shared objects (for example haspsrm_win32.dll for Win32 applications, refer dongle installation guide) must still be installed.

2. On Windows, the stand-alone SafeNet external license manager (hasp_rt.exe) must also be installed in the same directory as the application that accesses FLEXID9.

3. SafeNet driverless dongles are not currently accessible over a Windows remote desktop connection. For RDC support, Windows SafeNet drivers must still be installed. Flexera Software is working with SafeNet to obtain updated driverless dongles which are compatible with RDC.

(IOJ-1660103)

FLEXID9 memory leak

Prior to this release, memory was leaked each time FNP called the Safenet API to identify the FLEXID9 dongle. This issue has been addressed by a combination of fixes in FlexNet Publisher and fixes in the latest version of Safenet shared objects (haspsrm_*.dll/so/dylib). The updated SafeNet shared objects are now packaged in OS X, Linux and Windows FlexNet Publisher toolkits and lmadmin installers. Therefore, to prevent this memory leak, publishers must upgrade *both* the SafeNet shared objects and FlexNet Publisher components - such as the vendor daemon. (IOB-000063541)

Packaging Safenet external license manager

An unexpected Safenet error dialog, referring to the SafeNet '`hasp_cleanup`' API, appears when FLEXID9 Safenet runtime driver wasn't installed on the machine but the dynamic library (haspsrm_*.dll) was copied to System32/SysWow64 folder. This spurious dialog is prevented by the Safenet external license manager (hasp_rt.exe). The Safenet external license manger (hasp_rt.exe) is now packaged from v11.12.1.1 Windows toolkit and in the lmadmin installer. Place this file in the same folder as the FNP protected application (including lmhostid, lmtools, lmadmin, and the vendor daemon) to prevent the unexpected pop up dialog from Safenet. (IOC-000090914)

Known Issues in FlexNet Publisher (11.12.1.5) Service Pack 5

OS X lmadmin links with OpenSSL 1.0.1g

Recently, FlexNet Publisher components were upgraded to use OpenSSL 1.0.1h. The only exception to this is OS X lmadmin, where the upgrade for OpenSSL will trigger upgrades in other third-party libraries. This level of change is not appropriate for a service pack and OS X lmadmin OpenSSL therefore remains at v1.0.1g. The version of OpenSSL in OS X lmadmin will be upgraded to match the rest of FlexNet Publisher in a future release.

OpenSSL 1.0.1g does not contain the heartbleed bug. (FNP-9581)

Vendor daemon restart in revert-to-snapshot event

In the revert-to-snapshot event, the vendor daemon correctly shuts down with message "`Trusted storage binding change detected! Vendor daemon is being shutdown`" in server log. Before restarting the license server, the system clock may need to be synchronized with time server to avoid a subsequent unexpected restart of vendor daemon with message "`Lost connection to lmgrd, heartbeat timeout expired, exiting`" in server log. (IOA-000124628)

Supported Platforms

This service pack release supports: i86_n3, x64_n6, i86_lsb, x64_lsb, universal_mac10, hp700_u11i, hp64_u11i and it64_hp11i for SP5. For more details, see 11.12.1 Tier 1 release notes. Refer to url: http://www.flexerasoftware.com/support/eol/flexnet-publisher-end-of-life.htm for the latest information on supported platforms.