nShield Security World

nShield Security World v12.80 Release Notes

07 April 2024

Table of Contents

1. Introduction

These release notes apply to the release of version 12.80 of Security World Software for the nShield family of Hardware Security Modules (HSMs). They contain information specific to this release such as new features, defect fixes, and known issues.

Security World Software and CodeSafe Developer Software are for users of nShield Solo (PCI Express variants), nShield Connect, and nShield Edge.

The Release Notes may be updated with issues that have become known after this release has been made available. For the latest version, see the Entrust nShield Support portal.

Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

For the latest security notices and announcements please refer to Entrust nShield Announcements and Security Notices. The *Advisories* sub-section contains details of any advisories that have been announced for the nShield product range.

1.1. Purpose of Security World 12.80

Security World version 12.80 introduces enhancements as described in this document. It also corrects a number of defects that have been identified in earlier releases.

This release contains updates to the following products:

- Security World Software (including updated firmware and Connect image)
- CodeSafe Developer Software
- Remote Admin Client

If the v12.80 preview release of the nShield Connect image (v12.80.2) was used as part of preview release testing; it is required to upgrade the nShield Connect image to the later v12.80.4/v12.80.5 image that is available as part of this v12.80 release.

1.2. Versions of these Release Notes

Revision	Date	Description
1.5	2024-4-7	URL syntax fix for the HTML version. No content changes.
1.4	2022-3-25	Minor fixes and inclusion of link to security information portal in the Introduction
1.3	2022-2-9	Update to include details of the updated 12.80.5 Solo XC firmware and Connect XC image release. See Updates in 12.80.5 Release for more information on the release.
1.2	2022-1-18	• Addition of version of TSOP v8.0.0 to supported option pack list; see Option Pack support • Addition of known issue, NSE-43519, to section Known issues in Security World 12.80 • Fix to the directory path of the FIPS approved Connect images in the tables in section nShield Connect images • Fix to Python 3 development support to correct the name of the package that python 3 is in
1.1	2021-12-6	Fix to list of supported virtual environments in Supported virtual environments, to correctly list support for Microsoft Hyper-V Server 2016 and Microsoft Hyper-V Server 2019 (was listed as 2012 and 2016).
1.0	2021-11-23	Release notes for the first release of v12.80; v12.80.4
0.2	2021-10-21	Update to include 12.80 Connect image with 12.72.0 firmware. This is based on the same Connect image (12.80.2) that was previously released only with FIPS approved 12.50 firmware.
0.1	2021-09-29	Release notes for preview release of the 12.80 nShield Connect images

2. Product versions

2.1. Security World software versions

Version	Date	Description
v12.80.4	2021-11-23	First release of 12.80 Security World Software

2.2. CodeSafe Developer software versions

Version	Date	Description
v12.80.4	2021-11-23	First release of 12.80 CodeSafe Developer software.

2.3. Firmware and nShield Connect ISO versions

Version	Date	Description
v12.80.5	2022-2-9	Updated release of 12.80 Firmware and Connect ISO to include updated 12.80.5 Solo XC firmware and 12.80.5 latest Connect image. See Updates in 12.80.5 Release for more information.
v12.80.4	2021-11-23	First release of 12.80 Firmware and Connect ISO, including the release of firmware (12.80.2) and nShield Connect image (12.80.4) along with FIPS and CC approved firmware and Connect images.

2.4. nShield Firmware versions

Version	Date	Description
v12.80.5	2022-2-9	Updated version of 12.80 Solo XC firmware with required fixes. See Updates in 12.80.5 Release for more information.
v12.80.2	2021-11-23	First release of 12.80 Firmware for all HSMs containing the latest features and fixes.

2.5. nShield Connect image versions

Version	Date	Description
v12.80.5	2022-2-9	Updated version of latest Connect XC image with updated 12.80.5 Solo XC firmware. See Updates in 12.80.5 Release for more information
v12.80.4	2021-11-23	First release of nShield Connect images for 12.80 containing the latest features and fixes.
v12.80.2	2021-09-29	Initial release of 12.80 Connect images for preview release of 12.80 Connect features

3. Updates in 12.80.5 Release

12.80.5 delivers an updated Solo XC firmware and a nShield Connect XC image for use with the 12.80.4 clientside. The Firmware and Connect Image ISO has been updated to contain this updated firmware and Image. See Firmware, nShield Connect images, and certifications for details of the new firmware and nShield Connect image version numbers and location. Details of the changes included in this update are listed below.

3.1. Updated Solo XC Firmware

The Solo XC HSM contains a battery which is not used during normal powered operation. On shutdown the RTC operation is switched to be powered by the battery to ensure RTC is maintained when mains power is not present. To comply with certification, when the Solo XC is booted the HSM checks the battery voltage and if it is below a specified threshold the HSM will stop the boot and enter a SOS-B1 state. This would require the battery to be replaced prior to the HSM being able to start again.

NSE-41718 is an issue that was found in the 12.80.2 and 12.72.0 Solo XC firmware that caused the battery on the Solo XC to drain excessively on power down. If the Solo XC was then left with no mains power the battery could drain to below the required threshold which would cause the HSM to report SOS-B1 on next boot and would fail to start. In testing a Solo XC with 12.80.2 fw could have its battery drained below this threshold if it is left with no power for more than a few (~5) hours (this is dependent on the state of the battery in the specific Solo XC).

An updated version of 12.80 Solo XC firmware is available containing a defect fix for NSE-41718. The Solo XC version number is 12.80.5.

3.1.1. Upgrading the firmware

It is strongly advised that any Solo XC running 12.80.2 is upgraded to 12.80.5.

Prior to performing the upgrade it is possible to check on the state of the battery in the Solo XC. It is advisable to do this prior to performing the upgrade or power down if running the 12.80.2 firmware. The battery voltage on an HSM is reported in `stattree` as `CPUVoltage10`. Note that this voltage is only read once every 24 hours to help reduce battery drain.

```
-CPUVoltage10 3.02
```

If the battery voltage is shown as being below 2.7v it is possible that the battery needs to be replaced and should be done prior to powerdown or upgrade. Contact https://nshieldsupport.entrust.com for more information. Otherwise, upgrade the firmware as usual as instructed in the nShield Installation guide.

If the HSM does need to be powered off and left for a period of time prior to being upgraded to 12.80.5, it is recommended that following the power down and disconnection from mains, that the battery is removed to prevent the drain. This battery can then be re-inserted prior to putting the HSM back and upgrading the firmware. The RTC will then need to be reset following upgrade.

NSE-41325 is a related SOS-B1 issue that exists in 12.80 and previous releases that has been added as a known issue in Known issues from earlier Security World releases section.

3.2. Updated nShield Latest Connect XC Image

An updated version of the latest 12.80 Connect XC image is available containing the updated 12.80.5 Solo XC firmware. No other changes have been made to the Connect image itself and so the Connect Image with other versions of Solo XC and Solo+ firmware has not been updated and 12.80 continues to ship with 12.80.4 Connect images.

It is recommended that any Connect XC running 12.80.4 with 12.80.2 Solo XC firmware is upgraded to the 12.80.5 Connect image. A 12.80.4 Connect image that does not have the 12.80.2 firmware does not need to be upgraded.

4. Feature of Security World v12.80

4.1. IPv6 support on nShield Connect

IPv6 support was initially added to the nShield Connect as part of the Security World v12.10 release. This added basic IPv6 networking capability to the nShield Connect platform but the use of IPv4 was still required for normal usage such as crypto communication with the nShield Connect.

Security World v12.80 adds further IPv6 support to the nShield Connect by adding support for IPv6 networking to the following areas:

- Crypto communication - all communication between clients and the nShield Connect can be done using IPv6
- RFS - the Remote File System used by the nShield Connect can be identified using a static IPv6 address
- Configuration - It is possible to push a config file to the nShield Connect using a static IPv6 address

All of the client-side tools, the nShield Connect Serial Console, and the nShield Connect Front Panel have been updated to allow entry and use of IPv6 addresses to support the above changes.

As with IPv4 addresses, the IPv6 addresses used on the nShield Connect must be static to allow for continued communication between the HSM and the clients. The nShield Connect supports the use of SLAAC IPv6 addresses, but care must be taken to ensure that if these are used for nShield Connect identification that they remain static.

Client-side tools may now use a hostname that resolves to an IPv4 or IPv6 address instead of a static IP address to identify the nShield Connect.

SNMP and RA (Remote Administration) in the client-side, and NTP on the nShield Connect, still require the use of IPv4 addresses to function. The Connect's local Syslog logs can be pushed periodically to the RFS over IPv6, and IPv6 is also supported for audit logging to a remote Syslog server from the nShield Connect, but the Remote Syslog (remote_syslog configuration file section) feature for streaming the Connect's local logs to a remote Syslog server does not support IPv6.

Use of IPv6 addresses for these remaining tools will be added in a future release.

4.2. Network Bonding support on nShield Connect

Security World v12.80 adds support for the two nShield Connect network interfaces to be combined as a single logical bonded interface. This bond interface can be used in the following modes:

- Active backup mode
- 802.3ad mode (requires a switch that supports 802.3ad)

The bonding interface can be setup from the nShield Connect Front Panel, the nShield Connect Serial Console or by pushing a configuration file to the nShield Connect. The Connect Installation Guide provides full details of the setup required.

This network bonding support has not been setup to allow increased network performance.

4.3. AES-GCM support in the nCore API

Support for AES-GCM Wrapping mechanisms have been added to the firmware. This has been defined as a new nCore mechanism called `AESmGCM`. Later versions of Security World clientside software will add additional API support for this mechanism.

4.4. SHA-3 support in the nCore API

Support for SHA-3 hashing functions have been added to the firmware; these are defined in the nCore API as:

- SHA3b224Hash
- SHA3b256Hash
- SHA3b384Hash
- SHA3b512Hash

These have been implemented as defined in the FIPS-202 standard (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf). This is currently only available via the nCore API; additional API support will be added in future releases of Security World clientside software.

4.5. TUAK algorithm support in the nCore API

Support for TUAK algorithm has been added to the firmware. TUAK is a new mutual authentication and key generation algorithm published by the Third Generation Partnership Project (3GPP).

4.6. Key derivation to mechanisms with empty IVs

Several key derivation mechanisms are parameterized by an Initialization Vector `M_IV`. The mechanism contained in this IV may be restricted in a key's ACL, allowing users fine-grained control over key usage. However this mechanism could only be restricted to one that corresponded to a "generic" 64-, 128-, 192- and 256-bit IV types. This has been updated to allow it to be restricted to a mechanism with a completely empty IV.

4.7. Python 3 development support

A python 3 wheel file implementing the nfpython API was provided in Security World v12.60.5, which introduced support for Python 3 on both Windows and Linux and allowing python applications written in Python 3 to use nfpython API. Security World v12.80 extends this support by providing a python 3 interpreter as part of the Security World installation, further extending the use of Python 3 as a supported platform. This is installed in a `python3` directory (in `/opt/nfast` on Linux and `C:\Program Files\ncipher\nfast` on Windows).

The Python 3 version provided is Python 3.8.5 and it is contained in the nShield Hardware Support (`hwsp`) package.

The nShield developer guide contains a new Python 3 developer section containing details of how to write Python 3 applications using the nfpython API. The nShield CipherTools (`ctd`) package also contains example python 3 scripts.

Python2 is still included in the 12.80 installation and is installed as part of the core installation package into the `python` directory. This version of Python should continue to be used as the default version and should be used for running any nShield internal python scripts.

4.8. Entrust Branding

This release includes changes that update the branding to Entrust branding following the acquisition by Entrust. The changes in branding do not affect the product functionality.

5. Firmware, nShield Connect images, and certifications

Security World 12.80 does not include the firmware and nShield Connect image files in the standard Security World or CodeSafe ISOs. Instead, an nShield firmware and nShield Connect image ISO is available which contains all firmware and nShield Connect images supported by this release. This ISO can be obtained through contacting https://nshieldsupport.entrust.com (asking for product code `SW2187C-FW`).

5.1. Firmware

There is no change to the installation of the firmware in 12.80.

To install the updated firmware run the installed `loadrom` utility pointing at the required firmware file on the ISO (or copy the firmware from the ISO to a local location).

5.1.1. nShield Solo+ firmware

Type	Version	Description	Directory	VSN
CC Approved	2.55.1	The latest CC approved firmware for 11.72. This should be used with Security World 11.72.02 on the client host	`/firmware/2-55-1/ncx3p-29.nff`	29
FIPS Approved	12.50.8	The latest FIPS approved firmware released as part of the v12.50 release.	`/firmware/12-50-8/ncx3p-29.nff`	29
Latest	12.80.2	Latest firmware with features and defect fixes from v12.80 release.	`/firmware/12-80-2/ncx3p-29.nff`	29

The firmware monitor to use with the above nShield Solo+ firmware: `/firmware/2-60-1/ldb_ncx3p-26.nff`.

5.1.2. nShield Solo XC firmware

Type	Version	Description	Directory	VSN
CC Approved	12.60.15	The 12.60 firmware currently certified to the CMTS Common Criteria certification	`firmware/12-60-15/ncx5e-37.nff`	37
FIPS Approved	12.50.11	The latest FIPS approved firmware released as part of the v12.50 release.	`firmware/12-50-11/ncx5e-37.nff`	37
Latest	12.80.5	Latest firmware with features from v12.80 release.	`firmware/12-80-5/ncx5e-37.nff`	37

5.1.3. nShield Edge Firmware

There is no updated 12.80 firmware for the nShield Edge. Support for the Edge is still maintained for previous firmware releases.

Type	Version	Description	Directory	VSN
FIPS Approved	12.50.8	The latest FIPS approved firmware released as part of the v12.50 release.	`/firmware/12-50-8/ncx1z-29.nff`	29

The firmware monitor to use with the above nShield Edge firmware: `/firmware/2-50-16/ldb_ncx1z-24.nff`.

5.2. nShield Connect images

The nShield firmware and nShield Connect Image ISO includes 12.80 nShield Connect images that contain the Solo+ and Solo XC firmware described in nShield Solo+ firmware and nShield Solo XC firmware. The following nShield Connect images are available as part of the 12.80 release which contain the FIPS approved HSM firmware.

5.3. Install an nShield Connect image

Previously nShield Connect images were provided on the Security World Software ISO (as part of the `nhfw` package) which allowed them to be installed into `/opt/nfast/nethsm-firmware` ready to be installed onto the Connect image.

Now that these images are not on the Security World ISO these need to be manually copied into the correct location.

As part of the Security World installation the `/opt/nfast/nethsm-firmware` directory is created, but is empty.

Once the nShield Connect image that needs to be installed is chosen, the subdirectory, that is `12-80-2-fips`, and the image should be copied from the nShield firmware and nShield Connect ISO into the `/opt/nfast/nethsm-firmware` directory and installed onto the nShield Connect as usual.

5.3.1. nShield Connect+ images

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	12.45.1	nShield Connect image with CC approved 11.72 firmware	2.55.4	`nethsm-firmware/12-45-1/nCx3N.nff`	30
FIPS Approved	12.80.4	12.80 nShield Connect image with FIPS approved firmware	12.50.8	`nethsm-firmware/12-80-4-fips/nCx3N.nff`	31
Latest	12.80.4	12.80 nShield Connect image with latest 12.80 firmware	12.80.2	`nethsm-firmware/12-80-4-latest/nCx3N.nff`	31

5.3.2. nShield Connect CLX images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	12.80.4	12.80 nShield Connect image with FIPS approved firmware	12.50.8	`nethsm-firmware/12-80-4-fips/nCx3N.nff`	31
Latest	12.80.4	12.80 nShield Connect image with latest 12.80 firmware	12.80.2	`nethsm-firmware/12-80-4-latest/nCx3N.nff`	31

5.3.3. nShield Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	12.80.4	12.80 nShield Connect image with CC approved XC firmware	12.60.15	`nethsm-firmware/12-80-4-cc/nCx3N.nff`	31
Transition Image	12.50.4	12.50 nShield Connect image with FIPS firmware to support transition between old and latest Connect images. See Upgrade an nShield Connect XC image for more information.	3.4.2	`nethsm-firmware/12-50-4-fips/nCx3N.nff`	31
FIPS Approved	12.80.4	12.80 nShield Connect image with FIPS approved firmware	12.50.11	`nethsm-firmware/12-80-4-fips/nCx3N.nff`	31
Latest	12.80.5	12.80 nShield Connect image with latest 12.80 firmware	12.80.5	`nethsm-firmware/12-80-5-latest/nCx3N.nff`	31

6. Upgrade from previous releases

6.1. Install 12.80 Security World Software

Before installing this release, you must:

- Confirm that you have a current maintenance contract that licenses you to deploy upgrades on each nShield HSM and corresponding client operating system.
- Uninstall previous releases of Security World Software from the client machines.

For instructions, see the *Installation Guide* for your HSM.

6.2. Upgrade nShield Solo XC firmware

The following are important notes to observe when upgrading the Solo XC firmware to the latest version:

If the Solo XC HSM is installed with the earlier 3.3.10 firmware it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate version. Please contact nshield.support@entrust.com and request the firmware upgrade patch from 3.3.10 to 3.3.20.

If the nShield Solo XC HSM is installed with firmware earlier than 12.50.7, 12.50.2, 3.4.2 or 3.3.41 it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate version. Any of the firmware versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of firmware.

Whilst every effort is made to ensure nShield Solo XC firmware compatibility with all mainstream hardware and virtualized environments as well as operating systems there may be occasions where a particular configuration is not compatible (either through current version or after upgrading to a newer version of the firmware). Please contact nshield.support@entrust.com if you experience any issues following an upgrade or during integration activity.

6.3. Upgrade an nShield Connect XC image

If the nShield Connect XC HSM is installed with image earlier than 12.45, 12.46, 12.50.4, or 12.50.7 it cannot be upgraded directly to the latest nShield Connect image and needs to be first upgraded to an intermediate version. Any of the nShield Connect image versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of nShield Connect image.

7. Compatibility

7.1. Supported hardware

This release is targeted at deployments with any combination of the following nShield HSMs:

- nShield Solo XC
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect CLX (Base, Mid, High)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Edge
- nToken PCI Express "+" (NC2023E-000)

7.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

Operating System	Solo+	Solo XC	Connect	Edge
Microsoft Windows Server 2019 x64	Y	Y	Y	Y
Microsoft Windows Server 2019 Core x64	Y	Y	Y	**N**
Microsoft Windows Server 2016 x64	Y	Y	Y	Y
Microsoft Windows Server 2012 R2 x64	Y	Y	Y	Y
Microsoft Windows 10 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 6 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 7 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 8 x64	Y	Y	Y	Y
SUSE Enterprise Linux 12 x64	Y	Y	Y	Y
SUSE Enterprise Linux 15 x64	**N**	**N**	Y	**N**
Oracle Enterprise Linux 6.10 x64	Y	Y	Y	Y
Oracle Enterprise Linux 7.6 x64	Y	Y	Y	Y

Operating System	Solo+	Solo XC	Connect	Edge
Oracle Enterprise Linux 8 x64	Y	Y	Y	Y

Security World v12.80 Linux support is restricted to x86/x64 architectures. Additional mainstream x86/x64 based Linux distributions other than those listed above may be compatible, however Entrust cannot guarantee this compatibility.

7.3. Supported virtual environments

Operating System	Solo+	Solo XC	Connect	Edge
Microsoft Hyper-V Server 2016	N	Y	Y	N
Microsoft Hyper-V Server 2019	N	Y	Y	N
VMWare ESXi 6.5	N	Y	Y	N
Citrix XenServer 6.5	N	Y	Y	N
Citrix XenServer 8.2	N	Y	Y	N

7.4. Supported compilers for Microsoft Windows C developers

Security World v12.80 C libraries for Windows were built using Visual Studio 2017 and have been compiled with the SDL flag. This makes them incompatible with older versions of Visual Studio. This applies primarily to static libraries.

Microsoft Windows developers should upgrade to Visual Studio 2017.

8. Option Pack support

Option Pack	Compatible Version
Web Services Option Pack (WSOP)	To be confirmed
Time Stamp Option Pack (TSOP)	v8.0.0
Database Security Option Pack (nDSOP)	To be confirmed
Cloud Integration Option Pack (CIOP)	v2.2.1
nShield Container Option Pack (nSCOP)	To be confirmed

Contact nshield.support@entrust.com for further information about the availability of any option pack.

9. Defect fixes

9.1. Defect fixes in clientside software

Reference	Description
NSE-57	This release allows suppression of a potential flood of error messages in the event log when a CNG client requests unsupported properties. To enable this behavior either set the registry entry HKLM\Software\nCipher\CryptoNG\NoErrOnUnsupportedFlag to 1 or set the system environment variable NCCNG_NOERR_ON_UNSUPPORTED_FLAG to 1
NSE-2583	perfcheck no longer incorrectly prints "running tests" when the "--list" parameter is passed.
NSE-6930	Fixed an issue where the CSP Key Protection wizard would display the incorrect slot number.
NSE-26559	If there are symbolic links within the NFAST_KMDATA folder then the installation will pause. To rectify the issue remove any symbolic links that may exist within NFAST_KMDATA and re-run the installer.
NSE-28577	Skip comparing RemoteModule datalimit and agelimit flags as these are obsolete.
NSE-28619	Net-SNMP has been upgraded on v12.80 from v5.7.3 to the latest v5.9
NSE-28647	Multi-part HMAC operations in PKCS#11 were inefficient for small payloads.
NSE-28668	Keys that have been migrated from a version 1 World to a version 2 World using a key migration tool prior to 12.60 may fail to migrate successfully to a version 3 World. If the cardsets and keyfiles from the version 1 World still exist then they can be migrated directly to the version 3 World using the key migration tool delivered with this release.
NSE-30033	Some nfast applications do not report key information such as key name, hash, type and length when the application is run under preload. A new option --show -key-info has been added to preload for this purpose which will display key information when keys are loaded on modules.
NSE-30064	Previously CNG SignHash and VerifyHash operations with PKCS#1 padding did not check the validity of the input length parameter. These operations will now only accept input lengths matching the specified hash size.
NSE-31707	An issue where warning messages would pop up when building Java examples has been fixed.
NSE-32277	PKCS#11 applications are now able to start up or continue running when a module is unenrolled and reported 'Not Present'.

Reference	Description
NSE-32393	An issue on windows due to undocumented return value from the GetExtendedTcpTable has been addressed.
NSE-32407	The nShield Firmware ISO now contains details of the firmware and Connect images included on the ISO.
NSE-33005	The Linux install script now selects the latest compiled driver to install.
NSE-33508	Fixed an issue where the hardserver could potentially crash if a module was put into Maintenance mode.
NSE-33635	Error reporting from NFKM_cert_remoteshare was improved. Formerly it claimed that Remote Operator was disabled when used with a module that was not initialized into the security world.
NSE-33793	An issue where OCS or Softcard names including spaces would cause the migrate-world operation to fail has been resolved.
NSE-34560	Removed the obsolete method loadJNI in nCipherKM.jar.
NSE-35226	The validation of PSS and OAEP parameters could miss cases not supported by the module. If these occurred, incorrect results would be returned.
NSE-35653	An issue whereby using the java command adapter to import a key would fail in non CMTS worlds with InvalidParameter has been resolved.
NSE-35722	The nShield Linux driver source code files now include the GPL license header.
NSE-35822	CodeSafe reports the correct version number during installation.
NSE-35855	CKA_PUBLIC_EXPONENT is now optional in RSA key generation. It will default to 0x10001 (65537).
NSE-36061	The ncsnmp SNMP agent would crash when the NCIPHER-MIB::compName.1 entry was requested. This has now been resolved.
NSE-36617	An issue that affected the management of loaded objects on the module that could lead to memory exhaustion has been resolved.
NSE-36820	Fixed an issue where the hardserver could crash when pool mode commands were issued against an nShield Connect.
NSE-37030	The nShield PKCS#11 library will now recognize the CKA_ALWAYS_AUTHENTICATE attribute. It will always return false and attempts to set it are blocked. This provides support for clients that expect the attribute to be supported and did not handle its absence.
NSE-37385	Fixed an issue where Information-level log messages from the hardserver (nFast Server service) were not written to the Windows Event Log.

Reference	Description
NSE-37459	The nShield SNMP agent has been enhanced to perform queries for statistics and other information to the estate of HSMs in a parallel fashion. This can significantly improve the performance of the agent particularly in the presence of large numbers of HSMs and high latency connections.
NSE-38444	Fixed an issue where client applications could fail to connect to the nFast Server (hardserver) service if they lacked certain Windows privileges, e.g. in hardened hosting environments.
NSE-39194	The SECP256k1 curve is now supported by the NFKM Engine.
NSE-39209	Any GNU make Makefiles used to build SEE machines need to be updated to remove all reference to tokenise.o and tokenise.c Codesafe releases no longer includes makefiles. In the future, SEE compile/run tests should use the shipped CMake project files.
NSE-39862	Fixed an issue introduced in v12.70 where a hardserver client connection that continuously completely fills the HSM queues could prevent other connections from making progress with their commands.
NSE-40449	Fixed an issue where HMAC in CNG nCipher Primitive Provider could fail.
NSE-41587	Using the nShield PKCS#11 library with 12.50.11 or 12.50.8 FIPS firmware and later v12.70+ hostside software can lead to key generation and derive key operations failing with UnknownParameter when creating extractable secret keys. This has now been resolved so that these operations no longer fail when pre v12.70 firmware is used.

9.2. Defect fixes in Solo & Solo XC firmware

Defect fixes in the 12.80.5 Solo XC firmware:

Reference	Description
NSE-41718	Fix to Solo XC 12.80.2 firmware that caused excessive drain of the battery on the Solo XC HSM on shutdown, which could result in a SOS-B1 an next startup of the HSM.

Defect fixes in the 12.80.2 firmware:

Reference	Description
NSE-36108	GCM now limits the size of the plaintext to 68,719,476,704 bytes.
NSE-33978	Performance issues in Solo+ when Audit Logging is enabled that was introduced in v12.70 have been addressed

9.3. Defect fixes in Connect+, Connect CLX, and Connect XC images

Reference	Description
NSE-26595	Tab completion on the serial interface of the nShield Connect Serial Console now works
NSE-33839	Fixed an issue where updating some of the network configuration items on the nShield Connect front panel, the updated configuration was not pushed to the RFS
NSE-27699	Fixed an issue where updating the IP address via the serial console did not update the config file on the RFS
NSE-38379	Fixed an issue where, when adding IP routing information to the Connect via the Serial Console, error messages where not displayed when deleting or modifying a non-existing route entry.
NSE-1497	Can now use '--force' to deconfigure the specified Connect for the given IP address (without hkneti confirmation). i.e. 'nethsmenroll --remove --force <IP address>'

10. Known issues in Security World 12.80

See also Known issues from earlier Security World releases.

Reference	Description
NSE-41442	Earlier versions of nShield Java had a bug related to the order of clean up for unused or out-of-scope key objects and would sometimes return Status_UnknownID for operations during long running nCipherKM JCE and nCore Java applications. The cause of this issue has now been fixed. Java applications that perform operations directly with KeyID values rather than key objects may see Status_ObjectInUse errors unless keys, tokens, merged keys and channels are destroyed in the correct "LIFO" order. Attempting to destroy a key or other object that is referenced by another object will result in Status_ObjectInUse errors. Eg, If an application loads a key and creates a channel with that key, nCore Java will now return Status_ObjectInUse if the application attempts to destroy the key before destroying the channel using that key.
NSE-42172	The Java examples shipped with Security World Software are designed for use with later versions of Java (specifically Java version 8 and above). The Java examples may not work in earlier versions. Security World Software v12.80 continues to support Java versions 7, 8 and 11
NSE-39545	There is a performance regression in using ECDSA over SECP160r1 in the 12.80 Solo+ firmware. THis does not impact the Solo XC 12.80 firmware. Larger curve performance is also not impacted. If SECP160r1 is used it is recommended to not upgrade the firmware to 12.80 on the Solo+.
NSE-42034	Cmd_Encrypt does not properly populate the returned M_IV structured for Mech_AESmGCM. If an IV was supplied to Cmd_Encrypt then this value can be used instead. If no IV was supplied to Cmd_Encrypt then, for Mech_AESmGCM, the default chosen has taglen=16 and aad=the empty byteblock.
NSE-42346	The Edge Installation guide states it is not recommend to use a nShield Edge alongside other Entrust nShield HSMs on the same computer or VM. Use of a nShield Edge and a Solo on the same computer/VM will not work in the v12.80 release. If this use case is, against recommendation, used then Security World v12.80 should not be used.

Reference	Description
NSE-39031	In Security World v12.10 a compliance mode was added to the nShield Connect to allow compliance with USGv6 or IPv6 Ready requirements. This mode changes the settings for the nShield Connect firewall so that it will pass-through packets which are discarded in the normal Default mode. This behavior is required for compliance testing but is not recommended for normal use since allowing packets with invalid fields or parameters through the firewall increases the attack surface. This mode is known not to function correctly in the v12.80 Connect Image and should not be enabled.
NSE-41612	Downgrading an nShield Connect with the 12-80-3 Connect Image to an older version image with IPv6 networking configuration will require the nShield Connect to be factory reset following the upgrade. A new hardserver configuration file will also need to be created.
NSE-40445	Using traceroute from the front panel of the nShield Connect does not allow the network interface to use to be selected. When both interfaces are enabled, traceroute may select the incorrect interface and the traceroute will fail.
NSE-43519	12.80 clientside added support for IPv6 in the hardserver, however if IPv6 is disabled on the client machine the hardserver will fail to start. If IPv6 is disabled on the machine the following config item can be added to the Hardserver configuration file which will allow it to start: [server_remotecomms_ipv6] impath_port=0

11. Known issues from earlier Security World releases

These issues are still present in 12.80.

Reference	Description
NSE-41325	At power-up, the SoloXC HSM reads the voltage of its on-board battery. If the voltage reading is below the required threshold the module will enter a SOS-B1 low battery alarm state, and fail to start. Investigation has revealed that in very small number of servers, SoloXC may under-read the battery voltage at startup and incorrectly report a low battery alarm. Rebooting the server will usually return the SoloXC to normal operation. This issue is present in 12.7x versions of firmware as well as the recent 12.80 release. Therefore, if this issue has not been observed previously when running 12.7x firmware, it is unlikely to be seen with the more recent firmware builds. The issue can usually be avoided by configuring the server to maintain power to the module during a server main processor reboot or power cycle. Further investigation is ongoing to understand the server configuration that causes this issue and implement a fix. Note: This issue is different to the battery drain issue fixed as part of the 12.80.5 update release.
NSE-36364	In rare cases upgrading from v12.50.x images to later v12.70 or v12.80 images can result in the Connect becoming stuck in maint2 mode and report 'hardserver error' on the front panel. This can be resolved by initiating a factory reset and a repeat upgrade to the intended Connect image to complete the process.
NSE-28462	During key migration, if an incorrect OCS passphrase is entered, the tool will output the message: + Error: Cannot migrate security world. + Failed to load softcard <card_name> : wrong passphrase The 'Error: Cannot migrate security world' message is erroneous and can be ignored. The tool will continue and reprompt for the correct passphrase. Once the correct passphrase is entered the key migration will continue and complete successfully.
NSE-28606	nCipher Security do not recommend migrating keys to non-recoverable Worlds since it would then be impossible to migrate the keys in future should the need arise. If keys are migrated into a non-recoverable Wold then it is not possibly to verify OCS and softcard protected keys directly with nfkmverify. The OCS or softcards must be preloaded prior to attempting to verify the keys.

Reference	Description
NSE-24335	Note: This issue applies to 12.50.11 XC firmware only. As a result of work to improve the upgrade experience with Solo XC it is necessary to add the following lines to /etc/vmware/passthru.map for successful operation of Solo XC in an ESXi environment. # Solo XC 1957 082c link false
NSE-25477	If installing CAPI CSPs on Windows Server 2016 and 2019 do not select these as the default sChannel provider in the CSP wizards. If default sChannel is selected and the machine rebooted you will not be able to log in. It will be necessary to boot into safe mode and remove the CSPs as default sChannel providers.
NSE-23982	While resetting password if user enters incorrect password, cli prompt prints lone "I". This is where login handler program would print "Incorrect password for cli" message. Only "I" gets through the wire in time due to slow baud rate of the connection. This error is trivial and is only seen at the first log in during password reset.
NSE-23412	Customers should download at minimum CMAKE 3.9 for their RHEL distribution to be able to build the shipped examples.
NSE-25401	When installing 12.60 on a Dell XPS 8930 PC, a "Files in Use" screen may be displayed where it prompts to close down and restart Dell, Intel and NVIDIA applications. This can be ignored.
NSE-25626	Cancelling a Windows installation of the nShield Software with the "nShield Trusted Verification Device" component selected may leave the CyberJack Base Components installed on the machine. The user must restart their machine and uninstall the CyberJack Base Components manually via Add/Remove programs to completely uninstall.
NSE-22337	Users installing on a Pre-Windows 10 machine should download the Windows KB2999226 update to ensure the nShield Software will install correctly.
NSE-26559	If there are symbolic links within the NFAST_KMDATA folder then the installation will pause. To rectify the issue remove any symbolic links that may exist within NFAST_KMDATA and re-run the installer.
NSE-14406	In the Connect config file the remote_sys_log config entry implies multiple entries can be defined but only one remote syslog server can be configured.
NSE-14978	If Cmd_ChannelOpen is called without a key id an audit log message will be generated. This can occur if, for example, if Cmd_Hash is being used to hash a large amount of data. The nShield code translates this to opening a channel in Sign mode without a key. This would normally not be logged unless the key had the logkeyusage permission group flag. However, without a key the necessary checks cannot be performed and the Cmd_ChannelOpen is logged. This can be identified as a log entry without a key hash.

Reference	Description
NSE-14519	The enquiry utility in 12.0 client-side incorrectly reports 12.50/12.60 Connect modules as Failed. This is a reporting error in this utility only and does not affect other applications. To confirm the module is in fact usable it is possible to send a NoOp command with: nopclearfail -n -m 1
NSE-14362	Type 0 smart cards cannot be used in a FIPS level 3 enforced Security World (introduced in Security World v12.50). Contact Support if you need information on moving from type 0 smart cards to supported smart cards.
NSE-15284	With this release of the CodeSafe Developer Kit the build flags required for nShield Solo XC and nShield Connect XC have changed. It is essential that NF_CROSSCC is removed from all XC SEE Machine build configurations. See the examples in the developer kit for further details.
NSE-15762	Some instability has been seen in the CNG nShield Service Agent when HSMs report failure after being cleared.
NSE-15834	After disabling key recovery in a Security World (using killrecov), nfkmverify no longer verifies the Security World, reporting "ACL of NSO not of expected form". The Security World is still usable and key recovery has been disabled.