Release Notes

nShield Security World v12.72.3 Release Notes

Table of Contents

1. Introduction

These release notes apply to version 12.72.3 of nShield HSM firmware 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.

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.

1.1. Versions of these Release Notes

Date	Description
2024-07-25	Update to include details of updated 12.72 firmware for Solo XC (v12.72.3) and Edge (v12.72.2) as detailed in Update in Edge v12.72.2 and Solo XC v12.72.3. Firmware, nShield Connect images, and certifications has been updated with details of the new firmware and Connect images.
2024-01-24	PDF branding update. No content change to the product or the Release Notes.
2023-07-07	New Migrating to fips-140-2-level-3 SP800-56Ar3 compliant Security World section listing details of migrating from previous firmware versions. Update of warnings around use of SP800-56Ar3 worlds following the availability of new Remote Admin cards.
2023-04-19	Update to include support Security World v13.3 support
2022-12-16	Release notes for release of v12.72 firmware following FIPS approval

1.2. Product versions

1.2.1. Firmware

Version	Date	Description
v12.72.3	2024-06-28	Updated FIPS approved firmware for Solo XC
v12.72.2	2024-06-28	Updated FIPS approved firmware for Edge
v12.72.1	2022-10-16	FIPS approved firmware for Solo XC

Version	Date	Description
v12.72.0	2022-10-16	FIPS approved firmware for Edge and Solo+

1.2.2. Connect images

Version	Date	Description
v13.6.1	2024-06-28	13.6 Connect image containing the updated FIPS approved 12.72.3 Solo XC firmware.
v13.4.5	2023-12-15	13.4 Connect image containing the updated FIPS approved 12.72.2 Solo XC firmware and 12.72.0 Solo+ firmware.
v13.3.2	2023-03-31	13.3 Connect image containing the updated FIPS approved 12.72.2 Solo XC firmware and 12.72.0 Solo+ firmware.
v12.80.5	2022-10-16	12.80 Connect image containing the FIPS approved 12.72.1 Solo XC firmware and 12.72.0 Solo+ firmware.

2. Purpose of Security World v12.72

2.1. FIPS Approved Firmware release

nShield HSM firmware v12.72 introduces an updated version of the nShield HSM firmware that has been certified to FIPS 140-2 Level 2 and FIPS 140-2 Level 3.

This firmware update is for all nShield HSMs (Edge, Solo+ and Solo XC) and is based on the Security World v12.70 release. It introduces new features and changes mandated by NIST as part of the FIPS 140-2 standard. These changes are required for certification to be achieved and previous versions of firmware will move to the historical list at a time mandated by NIST.

It is important to read these release notes to understand the impact of the changes to the firmware and the best time to transition to this firmware.

An updated Connect image containing the v12.72 Solo+ and Solo XC firmware is also available.

2.2. Solo XC and Edge Firmware Update

Updated versions of FIPS 140-2 Certified 12.72 firmware for the Solo XC and nShield Edge have been created with additional fixes. Both of these firmware versions have been re-certified to FIPS 140-2 and are FIPS approved firmware. There is no update for the Solo+ firmware, whose latest version remains as v12.72.0. These new versions were first introduced as part of the Security World v13.6 update, which included this updated firmware.

Previous FIPS approved versions of Solo XC (v12.72.1) and nShield Edge (v12.72.0) nShield firmware remain FIPS approved and will continue to remain FIPS approved even when the new versions are certified. Upgrading to the latest versions of nShield firmware is only required if access to the latest changes in the nShield firmware are required.

2.3. FIPS Certificates

The following table lists the full details of the FIPS approved firmware versions and links to the security policy and FIPS certificate.

HSM	Certified Versions	FIPS Level	Certificate	Security Policy
Edge F2	v12.72.0 v12.72.2	140-2 Level 2	4331	Security Policy
Edge F3	v12.72.0 v12.72.2	140-2 Level 3	4332	Security Policy
Solo XC F2	v12.72.1 v12.72.3	140-2 Level 2	4333	Security Policy
Solo XC F3 Solo XC F3 for Connect XC HSMi	v12.72.1 v12.72.3	140-2 Level 2	4334	Security Policy
Solo XC F3 Solo XC F3 for Connect XC HSMi	v12.72.1 v12.72.3	140-2 Level 3	4335	Security Policy
Solo+ F2	v12.72.0	140-2 Level 2	4336	Security Policy
Solo+ F3 Solo+ F3 for Connect+, Connect CLX	v12.72.0	140-2 Level 2	4337	Security Policy
Solo+ F3 Solo+ F3 for Connect+, Connect CLX	v12.72.0	140-2 Level 3	4338	Security Policy

3. Update in Edge v12.72.2 and Solo XC v12.72.3

The updated release of v12.72 (v12.72.2 for Edge and v12.72.3 for Solo XC) contain the following updates:

3.1. Updated Remote Administration Card Support

Change first introduced in: v12.72.2

New Remote Administration Cards (v2) will shortly be introduced to replace the v1 cards. The v12.72.2 and v12.72.3 firmware introduce support for these new cards to ensure that once they are made available, not further firmware updates or certification is required.

v1.1 Remote Administration Cards currently remain as the latest version and can continue to be used with all v12.72 firmware.

3.2. CodeSafe Updates for Solo XC

Change first introduced in: v12.72.3

Updates have been made to CodeSafe in the XC product (Solo XC and Connect XC). The following fixes have been made to the v12.72.3 Solo XC firmware. Additional CodeSafe fixes have been made to the clientside and Connect image that is recommended to be used alongside these firmware fixes. These fixes are available in the v13.6 Security World release.

3.2.1. CodeSafe application MemAllocUser memory reporting

CodeSafe application memory usage via the `MemAllocUser` value in `stattree` was incorrectly reported in the Solo XC/Connect XC in the following cases:

- Incorrectly reporting 0 when the main thread of the application terminates but there are still background threads running (which is a common idiom in CSEE applications which call `SEElib_StartProcessorThreads()` followed by `ExitThread()` in the main thread)
- Failing to include memory usage of any child processes of the CodeSafe application in the total figure

Both of these issues (Defect NSE-32465) have been corrected.

Memory usage is also now reported based on `VmRSS` (resident set size) rather than `VmSize` (total virtual memory) as that better reflects true physical memory usage of the application. Note that memory usage reporting via `stattree` favors fast reporting, and that if applications need more accurate reporting they can use the `/proc` filesystem to report additional information from within their own application code, e.g. using information from `/proc/self/smaps`.

3.2.2. Performance of large commands and replies

There are two nShield firmware issues which affect the performance of processing of large commands and replies that are fixed in this release:

- Defect NSE-35968 caused a 1 second delay in an nCore reply being sent when the reply (total encoded size including overheads) was greater than 8192 bytes. This issue was first fixed in the v13.3 Solo XC firmware but has been backported to v12.72.3 (FIPS-approved). This affects any large reply messages sent to the host-side, including `Cmd_SEEJob` replies from a CodeSafe application.
- Defect NSE-60007 caused some inefficiency in the processing of replies to CodeSafe applications when the CodeSafe application provided a large buffer to receive the reply (as would be the case if the CodeSafe application intended to support the receipt of large replies to core jobs or SEEJobs)

4. Features of v12.72

The previous FIPS approved version of Edge and Solo+ firmware was 12.50.8 and for Solo XC was 12.50.11. This section details all the changes to the firmware that have been made since that release and are included in all versions of v12.72 firmware.

Also see the list of defect fixes listed in Known and fixed issues.

4.1. AES Keywrap with Padding

Change first introduced in: v12.60

Support for AESKeyWrap and AESKeyUnwrap with padding, compliant with NIST SP800-38F and RFC5649, has been added to the nShield firmware.

4.2. Generic ECC

Change first introduced in: v12.60

The key type `EC` has been added to the nShield firmware and is available via nCore. This key type can be used by both ECDH and ECDSA mechanisms allowing the same key to be used for both signing and key establishment. The intended use case for this is for when a static EC private key-establishment key is also required to sign a certificate request (CSR) for the (initial) certificate for the associated static public key-establishment key. Other use cases may be restricted by your security policy.

4.3. ECKA-EG mechanism

Change first introduced in: v12.60

Support for the ECKA-EG mechanism has been added to the nShield firmware and is available via nCore. Within nCore the mechanism is referred to as Elliptic Curve Diffie Hellman Key Agreement (ECDHKA). This mechanism is important for constrained IoT devices and is also part of the Elliptic Curve Integrated Encryption Scheme (ECIES).

4.4. ECKA and ECIES in the nCore API

Change first introduced in: v12.70

The following primitives have been added to the nCore API to support ECKA (Elliptic Curve

Key Agreement):

- `ECDHdKDF2`: ECDH (Elliptic-curve Diffie–Hellman) without cofactor + KDF2 key derivation
- `ECDHCdKDF2`: ECDH (Elliptic-curve Diffie–Hellman) with cofactor + KDF2 key derivation

The following derive mechanisms have been added to the nCore API to support key wrapping and unwrapping using ECIES (Elliptic Curve Integrated Encryption Scheme):

- `ECIESKeyWrap`
- `ECIESKeyUnwrap`

The key wrapping uses a XOR stream cipher and the SHA algorithm for hashing (SHA-1, SHA-224, and SHA-256/384/512).

4.5. CVN 18 Firmware Support

Change first introduced in: v12.70

This release now supports the VISA 18 scheme for truncated ARQC verification.

4.6. Hashing of Key Data in the firmware

Change first introduced in: v12.70

DeriveKey with RawEncrypt can now be provided a signing or hashing mechanism instead of an encrypt mechanism. In these cases, the raw key data is signed or hashed instead.

4.7. Removal of obsolete nCore mechanisms

Change first introduced in: v12.70

The following obsolete nCore mechanisms and key types have been disabled in the firmware: `KDPKeyWrapDES3`, `SignedKDPKeyWrapDES3`, `SSLRecordLayer`, `SSL3FinishedMsg`, `TLSFinishedMsg`, `SSL3withRSA`, `TLSwithRSA`, `SSL3withDH`, `TLSwithDH`, `RSAComponents`, `SSLMasterSecret`.

This impacts the following PKCS#11 attributes: `CKA_EXTRACTABLE`, `CKA_WRAP` and `CKA_UNWRAP`.

4.8. AES-GCM in the nCore API

Change first introduced in: v12.72

AES-GCM implementation was added to the firmware in the 12.60 firmware release but was subsequently removed due to issues with user-supplied IV's. v12.72 adds support for AES-GCM Wrapping mechanisms back to the firmware. However the IV used in encryption and wrapping is not user-suppliable and is generated by the firmware.

This has been defined as a new nCore mechanism called `AESmGCM`. This mechanism is available in both FIPS level-2 and level-3 modes.

4.9. FIPS SP800-90B

Change first introduced in: v12.72

Compliance with SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation (detailed https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf) has been added to the nShield firmware. This feature has no customer visible changes.

4.10. FIPS 186-4

Change first introduced in: v12.72

Compliance with FIPS 186-4 has been added to the nShield firmware for RSA key generation.

RSA key generation now always uses a FIPS 186-4 algorithm for key sizes greater than or equal to 1024 bits, so that all keys big enough to be FIPS-compliant are generated in a FIPS-compliant manner. Applications which do not explicitly request the `strong primes` flag, running in security worlds which do not have `strong primes` globally enabled, may experience a reduction in RSA key generation performance as a result.

4.11. FIPS SP800-56Ar3

Change first introduced in: v12.72

FIPS 140-2 Implementation Guidance D.1 mandates adoption of the SP800-56Ar3 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf) rules. The v12.72 firmware introduces new restrictions to the FIPS level-3 mode to reflect these new rules.

This change impacts the FIPS level-3 v3 (DLf3072s256mAEScSP800131Ar1) Security World modes (either newly created v3 worlds or v3 security worlds created with previous releases) loaded into the updated v12.72 firmware with the compliance mode enabled.

This compliance mode is enabled by the clientside when creating or loading the security world. At present this compliance mode is **not** enabled by default (due to implications with Remote Admin protocol and the associated Remote Admin cards discussed in Using the v12.72 release). To enable these restrictions the `--sp80056ar3` option can be supplied when creating/loading the security world. For example:

```
new-world --mode=fips-140-2-level-3 --sp80056ar3
```

In a future GA release, the clientside will be updated to enable this compliance mode by default and only security worlds with this enabled will be considered FIPS approved.

Compliance with the new compliant mode is shown by the `StrictSP80056Ar3` flag being present in the `active modes` entry in enquiry, as shown in the example below.

```
Module #2:
 enquiry reply flags  none
 enquiry reply level  Six
[...]
 supported KML types  DSAp1024s160 DSAp3072s256
 active modes         UseFIPSApprovedInternalMechanisms AlwaysUseStrongPrimes FIPSLevel3Enforcedv2
StrictSP80056Ar3
```

The other modes (`UseFIPSApprovedInternalMechanisms` and `FIPSLevel3Enforcedv2`) are also still required to show that the module is in a FIPS Level 3 approved mode.

Use of this compliance mode has implications on the Remote Administration Cards. See Using the v12.72 release for more information and read before using this feature.

5. Using the v12.72 release

This section details how to use the updated release.

5.1. nShield Firmware Image

See Firmware images for more information about updating the HSM to this FIPS approved version.

5.2. nShield Connect Image

The updated version of FIPS v12.72 firmware has been included in the latest versions of the nShield Connect Image. The nShield Connect image from the v12.80 Security World Release is provided as part of this FIPS release and is detailed in the Connect images section. Security World v13.3 and later versions of the nShield Connect image with v12.72 FW are also supported as a FIPS configuration.

This Connect image includes additional features that are included as part of those releases that are not detailed here and are not relevant to the FIPS firmware use. For more information about the Connect features see the relevant Release Notes. Contact nshield.support@entrust.com for more information.

5.3. nShield Clientside

There is no updated version of clientside software being released with v12.72. The following clientside versions can be used with the v12.72 firmware:

- Security World v12.70
- Security World v12.71
- Security World v12.80
- Security World v12.81
- Security World v13.3
- Security World v13.4
- Security World v13.6 (recommended)

These versions of clientside software do not enable to the SP800-56Ar3 restrictions by default as detailed in Features of v12.72. Whilst the above clientside allows these restrictions to be enabled on Security World loading or creation, care should be taken due to the impact on the nShield Remote Administration Cards. See below for more

information. A future Security World release will enable these restrictions by default.

See the related Security World Release Notes for details of the changes in the specific security world release. Security World versions later than v12.80 will continue to include support for the this FIPS approved firmware.

5.4. New nShield Remote Administration Protocol and Cards

Due to the changes made for SP800-56Ar3 new Remote Administration Cards are required to work with SP800-56Ar3 compliant Security Worlds. Creating SP800-56Ar3 compliant FIPS Level 3 Security Worlds will result in the current generation Remote Administration Cards not working with the Security World. Contact nshield.support@entrust.com for further details and to get the new cards and read Migrating to fips-140-2-level-3 SP800-56Ar3 compliant Security World for details of migrating to the new v1.1 cards.

Note that this is just impacting FIPS level-3 security world modes. The new v1.1 Remote Administration cards will work with both the old and new protocol (both old and SP800-56Ar3 compliant Security Worlds).

Security World Mode	Remote Admin Card
`unrestricted` (fips-140-level-2)	Works with current (v1.0) and new version (v1.1) of Remote Admin Cards; no update required
`fips-140-2-level-3`	New v1.1 Remote Admin Card required when used with SP800-56ar3 compliant Security World

6. Migrating to fips-140-2-level-3 SP800-56Ar3 compliant Security World

This section details how to migrate the existing Security World to a FIPS 140-2 Level 3 compliant Security World with SP80056Ar3 restrictions. It is assumed that the World being migrated was created as a FIPS 140-2 Level 3 Security World.

6.1. Loading the Security World

If this is the first time the Security World is being loaded into a FIPS Level 3 World with SP80056Ar3 restriction enabled on the module and any of the Cardsets (either ACS or any of the OCS cardsets) use the Remote Admin cards set, they must be replaced. See below for more information on migrating the different cardset types.

The cardsets need to be migrated to new cards **before** migrating to a Security World with SP80056Ar3 restrictions enabled.

After any cardsets are migrated the existing Security World can be loaded into the new 12.72 FW using `new-world -l --sp80056ar3`.

6.1.1. Administrator Cardset Upgrade

If the ACS uses Remote Admin cards then it must be replaced with new v1.1 Remote Admin Cards.

- Use `racs` to create a new ACS, using new v1.1 Remote Admin cards.
- Verify that the new ACS can be used to load the world and recover keys.
- Archive/dispose of the old ACS, according to organization policy.

6.1.2. Operator Cardset Upgrade

If any OCS uses Remote Admin cards then it must be replaced with new v1.1 Remote Admin cards.

To do this using key recovery:

- Create all new operator cardsets required, using new v1.1 Remote Admin cards.
- Use `rocs` to migrate keys protected by the each old OCS to the corresponding new OCS.

- Verify that each new OCS can be used to load the keys it protects.
- Archive/dispose of the old OCS, according to organization policy.

6.1.2.1. Non-Recoverable Keys

Keys that aren't recoverable but are protected by Remote Admin cards cannot be migrated to the new v1.1 Remote Admin cards.

You have the following options:

- Retire existing keys and generate new ones.
- Do not upgrade to v12.72 or later firmware. From 2025 onward, your module's FIPS-140 certificate will be Historical.
- Upgrade to v12.72 or later firmware, but use the `--no-sp80056ar3` option. Your module will not be in a FIPS-140 level 3 compliant configuration.

7. Firmware, nShield Connect images, and certifications

This section contains details of the updated firmware and Connect images being made as part of the 12.72 FIPS release.

7.1. Firmware images

There is no change to the installation of the firmware in v12.72.

To install the updated firmware run the installed `loadrom` utility pointing at the required firmware file.

7.1.1. Solo+ firmware

Type	Version	Description	Directory	VSN
FIPS Approved	12.72.0	FIPS approved firmware released as part of the v12.70 release. Released as part of the Security World v13.3 release.	`/firmware/12-72-0/ncx3p-29.nff`	29

7.1.2. Edge Firmware

Type	Version	Description	Directory	VSN
FIPS Approved	12.72.0	FIPS approved firmware released as part of the v12.70 release. Released as part of the Security World v13.3 release.	`/firmware/12-72-0/ncx1z-29.nff`	29
FIPS Approved	12.72.2	Updated FIPS approved firmware with changes defined in Update in Edge v12.72.2 and Solo XC v12.72.3. Released as part of the Security World v13.6 release.	`/firmware/12-72-2/ncx1z-29.nff`	29

7.1.3. Solo XC firmware

Type	Version	Description	Directory	VSN
FIPS Approved	12.72.1	FIPS approved firmware released as part of the v12.70 release. Released as part of the Security World v13.3 release.	`firmware/12-72-1/ncx5e-37.nff`	37
FIPS Approved	12.72.3	Updated FIPS approved firmware with changes defined in Update in Edge v12.72.2 and Solo XC v12.72.3. Released as part of the Security World v13.6 release.	`firmware/12-72-3/ncx5e-37.nff`	37

7.2. Connect images

All major Security World releases contain an updated Connect image containing the FIPS approved firmware. The following section contains details of the recent Connect images containing the 12.72 FIPS firmware. See the Security World release notes from that release for additional information about the changes to the Connect image.

7.2.1. Install an 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 it is empty.

Once the nShield Connect image that needs to be installed is chosen, the subdirectory, that is `12-80-5-fipspending`, and the image should be copied into the `/opt/nfast/nethsm-firmware` directory and installed onto the nShield Connect as usual.

The paths below for the 12.80 Connect image is in a folder called `fipspending`, however this image is the FIPS approved version containing the FIPS approved firmware.

7.3. Connect+ images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	12.80.5	12.80 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/12-80-5-fipspending/nCx3N.nff`	31
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-3-2/nCx3N.nff`	32
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-4-5/nCx3N.nff`	32

7.4. Connect CLX images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	12.80.5	12.80 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/12-80-5-fipspending/nCx3N.nff`	31
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-3-2/nCx3N.nff`	32
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-4-5/nCx3N.nff`	32

7.5. Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	12.80.5	12.80 nShield Connect image with FIPS approved firmware	12.72.1	`nethsm-firmware/12-80-5-fipspending/nCx3N.nff`	31
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.1	`nethsm-firmware/fips-all-13-3-2/nCx3N.nff`	32
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.1	`nethsm-firmware/fips-all-13-4-5/nCx3N.nff`	32
FIPS Approved	13.6.1	13.6 nShield Connect image with updated FIPS approved firmware	12.72.3	`nethsm-firmware/fips-all-13-6-1/nCx3N.nff`	32

8. Upgrade from previous releases

8.1. Upgrade 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 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 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.

9. Upgrade a 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.

10. Compatibility

10.1. Supported hardware

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

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

10.2. Supported Security World Software

The following clientside versions can be used with the v12.72 firmware:

- Security World v12.70
- Security World v12.71
- Security World v12.80
- Security World v12.81
- Security World v13.3
- Security World v13.6 (recommended)

Security World versions later than v13.6 will continue to include support for the this FIPS approved firmware. It is advised to use the latest version of Security World Software (v13.6) to ensure latest fixes and security updates are used.

See the related Security World Release Notes for details of compatibility support.

11. Known and fixed issues

The table below lists known and fixed issues in the v12.72 firmware. For details of known and fixed issues in the Connect or clientside used with this firmware, consult the relevant Security World release notes for that release.

Reference	Scope	Status	Description
NSE-32465	Firmware	Resolved	Fixed issues with reporting of CodeSafe application memory usage in MemAllocUser stattree value in Solo XC and Connect XC: * Incorrectly reporting 0 when the main thread of the application terminates but there are still background threads running (which is a common idiom in applications using SEElib_StartProcessorThreads) * Failing to include memory usage of any child processes of the CodeSafe application Memory usage is also now reported based on VmRSS (resident set size) rather than VmSize (total virtual memory) as that better reflects true physical memory usage of the application. Note that memory usage reporting via stattree favours fast reporting, and that if applications need more accurate reporting they can use the /proc filesystem to report additional information from within their own application code, e.g. using information from /proc/self/smaps. **Resolved** in 12.72.3 firmware.
NSE-41718	Firmware (Solo XC only)	Resolved	Fix to Solo XC firmware (versions v12.70.8, v12.72.0 and v12.80.2) 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. **Resolved** in 12.72 Solo XC firmware.
NSE-30626	Firmware	Resolved	Fixed an issue where a DeriveKey operation using SHA1 with DeriveMech_RawEncrypt and Mech_RSApPKCS1OAEP was incorrectly disabled in a FIPS 140-2 Level 3 Security World. It is now permitted. **Resolved** in 12.72 firmware.
NSE-28905	Firmware	Resolved	Fixed DES parity bits not being set properly when generating one of the DES key variants using the ECDHKA key derivation mechanism. This issue caused the key derivation operation to fail. **Resolved** in 12.72 firmware.

Reference	Scope	Status	Description
NSE-28374	Firmware	Resolved	DeriveMech_ECDHKA was expanded to support ECPrivate and ECPublic keys as well as ECDHPrivate and ECDHPublic. **Resolved** in 12.72 firmware.
NSE-28373	Firmware	Resolved	It is now possible to specify KAPrimitive_Any, and IESCipherMode_Any, in an Act_DeriveKey or Act_DeriveKeyEx action in a key ACL. Doing so will permit ECDHKA or ECIES operations with any support key agreement primitive, or cipher mode, respectively. **Resolved** in 12.72 firmware.
NSE-2804	Firmware	Resolved	An issue where the nvram-sw command could not delete persistent NVRAM files was fixed. **Resolved** in 12.72 firmware.
NSE-34615	Firmware (Solo XC only)	Resolved	An issue was found on the v12.70.3 Connect XC image running the latest v12.70.2 Solo XC firmware which caused the HSM to halt cryptographic operations on some HMSs after a long running time (20+ days). This issue was found to be present in the v12.70.2 Solo XC firmware (although the issue has never been reproduced outside of a Connect HSM). Improvements have been added to the firmware and an updated Solo XC firmware and Connect image containing that firmware is available as 12.70.8. This issue does not impact Solo+ firmware. **Resolved** in 12.72 Solo XC firmware.
NSE-31968	Firmware	Resolved	The lifetime of an nCore challenge was raised from 30 seconds to 120 seconds, in order to improve the reliability of challenge based operations and impath connection establishment. **Resolved** in 12.72 firmware.
NSE-30880	Firmware	Resolved	The HSM firmware now properly rejects unsupported or illegal combinations of flags set with the InitialiseUnitEx and/or SetNSOPerms commands while the HSM is in Initialisation mode. This will not affect the behavior of any Security Worlds created or loaded using the new-world utility. **Resolved** in 12.72 firmware.

Reference	Scope	Status	Description
NSE-24229	Firmware	Resolved	The 'Payshield' feature enable bit has been renamed to 'CANActivation'. **Resolved** in 12.72 firmware.
NSE-19954	Firmware (Solo XC only)	Resolved	Solo XC modules in Maintenance mode no longer report an InvalidState error when sent a Cmd_NoOp command. **Resolved** in 12.72 Solo XC firmware.
NSE-4583	Firmware	Resolved	A bug which can cause the 'slotinfo' utility to report the smart card type incorrectly has been fixed. **Resolved** in 12.72 firmware.
NSE-9958	Firmware (Solo XC only)	Resolved	The RTC on Solo XC now delivers results with 1ms resolution, improved from the previous 1 second resolution. **Resolved** in 12.72 firmware.
NSE-16042	Firmware (Solo XC only)	Resolved	nShield XC HSMs could infrequently stop responding to requests for cryptographic operations. Failure was independent of cryptographic function, HSM load, or deployment. Although symptoms varied, it was likely that the hardserver logs would include a message of the form hardware error was '\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF'. On Connect XC, the front panel would display 'HSM Failed'. Depending on the variant (Solo XC or Connect XC) the HSM may have fully recovered without intervention, or may have required a full cold start reboot (eg via the Connect XC power switch) to return it to an operational state. The issue is resolved in the 12.50.11 and the 12.60.2 firmware release. **Resolved** in 12.72 firmware.
NSE-14444	Firmware (Solo XC only)	Resolved	The Solo XC no longer locks up and causes a system panic on Solaris 11 and Oracle SPARC T7-1 servers. **Resolved** in 12.72 Solo XC firmware.
NSE-15569	Firmware	Resolved	The HSM could lock-up when a very high number of dynamic slots were configured. **Resolved** in 12.72 firmware.

Reference	Scope	Status	Description
NSE-16572	Firmware	Resolved	The AESKeyWrap mechanism optionally allows the caller to specify an IV value. However, NIST SP800-38F mandates that this value is fixed. Therefore, in Strict FIPS mode the firmware will now reject commands which specify an IV value. **Resolved** in 12.72 firmware.
NSE-19400	Firmware	Resolved	The obsolete mechanisms SSL3withDHEx and TLSwithDHEx have been removed from the firmware. **Resolved** in 12.72 firmware.
NSE-22054	Firmware (Solo XC only)	Resolved	The Solo XC now retains its RTC time following a reboot. **Resolved** in 12.72 Solo XC firmware.
NSE-22187	Firmware (Solo XC only)	Resolved	CodeSafe applications running on a Solo XC or a Connect XC with high CPU usage would be terminated by the HSM's supervisory functions. This is no longer the case. **Resolved** in 12.72 Solo XC firmware.
NSE-22572	Firmware	Resolved	The HSM now correctly pads the Z parameter in ECCMQV (provided via the DeriveMech_ECCMQV nCore command). NSE-23623 The HSM now ensures that correct ticket references are provided to the host via the Cmd_RedeemTicket nCore command. **Resolved** in 12.72 firmware.
NSE-23661	Firmware	Resolved	A firmware bug which caused a spurious NVRAM file to be visible when Audit Logging was enabled has been fixed. **Resolved** in 12.72 firmware.
NSE-23721	Firmware	Resolved	The Vendor ID field appearing in CEF log messages from the HSM now appears as 'nCipher Security'. **Resolved** in 12.72 firmware.

Reference	Scope	Status	Description
NSE-25299	Firmware	Resolved	An Impath key exchange would fail if the Elliptic Curve (EC) feature was not enabled on the modules involved in the key exchange. This has been corrected so that the key exchange will succeed even without the EC feature enabled. **Resolved** in 12.72 firmware.
NSE-42034	Firmware	Open	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-41325	Firmware (Solo XC only)	Open	At power-up, the Solo XC 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.
NSE-14978	Firmware	Open	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.
NSE-14362	Firmware	Open	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.