nShield Security World

nShield Security World v13.9.5 Release Notes

23 April 2026

Table of Contents

1. Introduction

These release notes apply to the release of version 13.9.5 of Security World for the nShield family of Hardware Security Modules (HSMs).

These release notes contain information specific to this release such as new features, defect fixes, and known issues. They may be updated with issues that have become known after this release has been made available. For the latest version, see https://trustedcare.entrust.com/. Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

We continuously improve the user documents and update them after the general availability (GA) release. Changes in the document set are recorded in these release notes and are published at https://nshielddocs.entrust.com.

1.1. Updated nShield Software Release Policy

Entrust has recently introduced an update to the nShield Software release policy to better define the type of release and the associated update and support policy. As part of this, the concept of Long Term Support (LTS) and Standard Term Support (STS) software releases has been introduced, with each software release being either a LTS or STS release.

For more information on the software release policy, see the nShield Security World Release Information. Alternatively contact https://trustedcare.entrust.com/ for more information.

1.2. Purpose of Security World v13.9

Security World version v13.9 introduces new features and enhancements as described in Features of Security World v13.9 STS Release 3. It also corrects a number of defects that have been identified in earlier releases.

Security World 13.9.5 is a **Standard-Term Supported (STS)** release. This release is designed to give early access to new nShield features and has a shorter support period.
For long-term support (LTS), frequent stability updates and certified firmware, it is recommended to use the v13.6 Long-Term Support release. See the nShield Security World Release Information for details of the supported versions and the STS & LTS policy.

This release contains updates to the following products:

- Updated firmware for nShield 5s (no incremental change in v13.9 STS Release 3 compared to Release 2)
- Updated Connect images for nShield 5c and Connect XC (including further updates in v13.9 STS Release 3)

1.3. Versions of these Release Notes

Revision	Date	Description
1.0	2026-04-24	Release notes for the release of v13.9.5, Security World v13.9 STS Release 3.

2. Product versions

2.1. Security World software versions

Version	Date	Description
v13.9.5	2026-04-24	Full Release of the 13.9.5 Linux and Windows ISOs.

2.2. CodeSafe Developer software versions

Version	Date	Description
v13.9.5	2026-04-24	Full Release of the 13.9.5 CodeSafe Linux and Windows ISOs.

2.3. Firmware and Connect ISO versions

Version	Date	Description
v13.9.5	2026-04-24	Full Release of the 13.9.5 FW ISO including the updated 13.9 Connect images and the Security World v13.9 STS Release 2 13.8 firmware.

2.4. Connect image versions

Version	Date	Description
v13.9.5	2026-04-24	Full Release of 13.9 images for nShield 5c and nShield Connect XC HSMs containing the latest features and fixes.

3. Features of Security World v13.9 STS Release 3

3.1. New v13.9.5 Connect Images

Refer to Connect images for more information on the new v13.9.5 Connect images.

Refer to Known and fixed issues for more information on fixed issues in the new v13.9.5 Connect images.

3.1.1. Unset module RTC upgrade issue on Connect 5c units

v13.9 images are unaffected by this issue as it is no longer possible to upgrade to a v13.9 image with an unset RTC. An appropriate error will be displayed if the RTC is unset during the upgrade process and the nShield 5c RTC will need to be set to continue with the upgrade.

Connect 5c only Due to NSE-69020 if the nShield 5c unit RTC is not set it will result in an upgrade failure.

The following **nShield 5c** images are impacted by NSE-69020:

Release	nShield 5c Version
Security World v13.6.3 LTS Release	v13.6.1
Security World v13.6.5 LTS Update 1	v13.6.4
Security World v13.6.8 LTS Update 2	v13.6.7
Security World v13.7.3 STS Release 1	v13.7.1

To determine if your **nShield 5c** unit has the RTC set correctly, execute the `ncdate` command against the target nShield 5c unit.

A nShield 5c with the correct RTC date and time set should display a variance of the following:

```
# ncdate -m1
Local time is 07:03:54.943 2025.03.12
```

An nShield 5c with an incorrect RTC date and time will display the following variance:

```
# ncdate -m1
Local time is 07:03:54.943 1970.03.12
```

Please contact nshield.support@entrust.com if the RTC for your **nShield 5c** unit is incorrectly set for more assistance.

3.2. CodeSafe 5: Auto-load from 5c (Connect) config and multi-client multiplexing of SEEJobs (NSE-71048)

Security World v13.9 STS Release 3 introduces support for the automatic loading of CodeSafe 5 applications directly from the nShield 5c appliance.

- CodeSafe 5 applications can now be started directly via the nShield 5c (Connect) config file, with CS5 and Developer ID files pulled automatically from the RFS.
- Applications specified in the nShield 5c config are started automatically when the nShield 5c is rebooted or module cleared.
- CodeSafe 5 applications loaded directly from the nShield 5c can make their SEE World ID available as a published object, enabling multiple remote client machines to communicate with the same CodeSafe 5 application via the SEEJobs protocol.

The following instructions describe how to use the nShield 5c with this additional CodeSafe 5 functionality.

Install the latest nShield host-side software and run the `rfs-setup` utility to allow the nShield 5c to retrieve the required Developer ID certificate(s) from the RFS's `cscerts` volume. If you have previously configured your RFS prior to this release, `rfs-setup` must be run again to add the permission for this new volume.

Build and sign the CodeSafe 5 image as normal.

Permit the nShield 5c to have a configuration file pushed from a remote machine. By default, the configuration file can be pushed from the RFS machine, provided it is authenticated. To allow another remote machine to push configuration, use the 5c's `Client config push` menu from its front panel UI (menu 1-1-6-2). Configure the nShield 5c to append its logs (hardserver and system logs) to the RFS once per minute in order to get timely feedback on CodeSafe 5 configuration operations. Alternatively, you can configure a remote UDP syslog server to receive streamed logs, or a privileged client can obtain on demand the most recent logs that have not yet been pushed to the RFS by using the following commands (replace `-m1` with the module number of the 5c):

```
appliance-cli -m1 getservlog --log hardserver
```

```
appliance-cli -m1 getservlog --log system
```

Copy the Developer ID certificate(s) required by the CodeSafe 5 application to this directory on the RFS `/opt/nfast/kmdata/cscerts` (Linux) or `C:\ProgramData\nCipher\Key Management Data\cscerts` (Windows).

Copy the CodeSafe 5 image into `/opt/nfast/custom-seemachines` (Linux) or `C:\Program Files\nCipher\nfast\custom-seemachines` (Windows).

Copy the original nShield 5c configuration file `/opt/nfast/kmdata/hsm-<ESN>/config/config` (Linux) or `C:\ProgramData\nCipher\Key Management Data\hsm-<ESN>\config\config` (Windows) to `config.new` in the same directory.

Edit the `[codesafe]` section of the nShield 5c `config.new` file on the RFS so that it contains the following entries (replace `cs5app.cs5` with the actual CodeSafe 5 application filename; this file will be pulled from the `custom-seemachines` volume on the RFS, so use only the filename, not the path):

```
[codesafe]
image_file=cs5app.cs5
worldid_pubname=mysee
pull_rfs=yes
```

Push the configuration to the nShield 5c (note: this will stop the nShield 5c's CodeSafe 5 application if one is currently running): On Linux:

```
cfg-pushnethsm -a <nShield 5c IP address> -m <module number> /opt/nfast/kmdata/hsm-<ESN>/config/config.new
```

On Windows:

```
cfg-pushnethsm -a <nShield 5c IP address> -m <module number> "C:\ProgramData\nCipher\Key Management Data\hsm-
<ESN>\config\config.new"
```

Wait for one minute for the CodeSafe 5 application to be automatically transferred from the RFS to the nShield 5c.

Clear the nShield 5c:

```
nopclearfail -m <module number> --clear --wait
```

Wait for the CodeSafe 5 application to be automatically loaded and started. Check the nShield 5c's hardserver logs on the RFS for the following message, which indicates that the CodeSafe 5 application has been started:

```
Startup: hsc_codesafe:INFO: READY: /config/see/machine/seemachine.cs5 running on <ESN> (#1); SEE World ID
published as mysee; appliance-cli -m <module number> cs5 getlog <UUID> to retrieve logs
```

Note that `seemachine.cs5`, which is mentioned in the log message, is the internal filename used after the file has been copied from the RFS. The file that is copied is the file on the RFS whose original filename is specified in the `config` file.

Clients can now communicate with the CodeSafe 5 application.

3.3. CodeSafe 5: Support standard nShield APIs (NSE-56426)

Security World v13.9 STS Release 3 introduces support for the following libraries in CodeSafe 5:

- **C Generic Stub (the NFastApp API for nCore)**
  - Static library: `/opt/nfast/c/csd5/lib-ppc64-linux-musl/libnfstub.a`
  - Include directory (e.g. for `nfastapp.h`): `/opt/nfast/c/csd5/include-see/hilibs`
- **NFKM (the Security World API)**
  - Static library: `/opt/nfast/c/csd5/lib-ppc64-linux-musl/libnfkm.a`
  - Include directory (e.g. for `nfkm.h`): `/opt/nfast/c/csd5/include-see/sworld`
- **`nfpython` and `nfkm` modules in Python**

3.3.1. Python module removal

Code using `nshield.ipcdaemon.seeapi` must be updated to use `nfpython` or `nfkm`.

The `nshield.ipcdaemon.seeapi` module has been removed. The `nfpython` (or `nfkm`) module should be used instead. These modules are consistent with client-side applications for nShield, so there is no longer a CodeSafe-specific module.

You should update any old code using `nshield.ipcdaemon.seeapi` to use `nfpython`, for example:

Old code

```
from nshield.ipcdaemon.seeapi import SEEAPI
conn = SEEAPI()
conn.connect()
reply = conn.transact(command)
```

Updated code

```
import nfpython
conn = nfpython.connection()
reply = conn.transact(command)
```

3.3.2. Examples

- The `/opt/nfast/c/csd5/examples/netsee/hellonshield` example has been added to show use of nCore and NFKM from C
- The `/opt/nfast/python3/csd5/examples/webserver/` example has been updated to show use of nCore and NFKM from Python

These examples also show how the `extra-packages-conf.json` file can be used to pull in the contents of `${NFAST_KMLOCAL}` and `${NFAST_CARDLIST}` to pull Security World files from the local environment into the CodeSafe 5 container that is built so that it is accessible to the NFKM library.

3.3.3. Combining SEElib with C Generic Stub (NFastApp) or NFKM

When combining SEElib with NFastApp or NFKM, always link against `libnfstub.a` instead of `seelib.a`.

The traditional CodeSafe 5 SEElib library continues to exist as the stand-alone library `seelib.a`.

This static library is not compatible with `libnfstub.a` or `libnfkm.a`.

For users who combine the use of SEElib (`SEElib_*` functions) with the `NFastApp_*` functions in the C Generic Stub and/or the NFKM APIs, the C Generic Stub static library `libnfstub.a` now also includes the full SEElib API.

If the goal is to migrate use of `SEElib_Transact` to `NFastApp_Transact` for consistency with client-side application code whilst still retaining support for SEEJobs, or if SEElib is being used primarily but NFKM library must also be used in the same application, then `libnfstub.a` must be used instead. This provides all the SEElib symbols in a form compatible with `libnfstub.a` and `libnfkm.a`. `seelib.a` must not be linked against in this case. The usual `seelib.h` header should continue to be used to obtain the declarations, but if also including C Generic Stub (such as `nfastapp.h`) or NFKM headers (such as `nfkm.h`), they should be included before `seelib.h`.

If `SEElib_init()` is called in the `libnfstub.a` implementation, it will initialize an `NFast_AppHandle` internally which is configured to marshal `M_Bignum` objects in the form defined by

`struct NFast_Bignum` in the `seelib.h` header, i.e. as a `M_ByteBlock` containing a little-endian representation of the value. This makes the default marshalling behaviour and `struct` representation of objects when migrating existing SEElib code from `seelib.a` to `libnfstub.a` identical.

In order to support inter-operation with other `NFastApp` use-cases, new APIs `SEElib_init_NFastApp()` and `SEElib_init_NFastApp_default()` have been added in `seelib.h` that can be called instead of `SEElib_init()` if required. These new functions are declared if `nfastapp.h` is included before `seelib.h`. `SEElib_init_NFastApp()` allows initialization of SEElib with the caller's own `NFast_AppHandle`, allowing the caller to precisely control the NFastApp initialization. `SEElib_init_NFastApp_default()` initializes the SEElib library with the default NFastApp Bignum implementation defined in `nfastapp-bignum.h`. This provides maximum compatibility with typical default NFastApp initialization that would be used in most client-side application code that is being migrated to CodeSafe 5. If `nfastapp-bignum.h` is being used, it should be included before `seelib.h`.

If "manual" marshalling or unmarshalling of nCore types is performed using functions such as `NF_Marshal_CertificateList` or `NF_Unmarshal_CertificateList`, the `struct NF_UserData *` context in the `NF_Marshal_Context.u` or `NF_Unmarshal_Context.u` field is set to `NULL` in traditional `seelib.a` applications. If using marshalling or unmarshalling functions when linking against `libnfstub.a`, the `struct NF_UserData * u;` field must now be set to a valid Generic Stub object. This should either be obtained in the usual manner using the `NFastApp` APIs, or if using the `SEElib` initialization extensions, it can be obtained using the new `SEElib_GetUserData()` function. When using `seelib.a`, `SEElib_GetUserData()` will always return `NULL` as it is not applicable for the implementation of the marshalling and unmarshalling functions in that version of the library.

3.4. CodeSafe 5: SEEJobs Optimizations (NSE-77084)

Security World v13.9 STS Release 3 includes optimizations for CodeSafe 5 SEEJobs in SEElib. A rebuild of the CodeSafe 5 application with the updated CodeSafe SDK is required to obtain this optimization.

A new feature has also been added to the Security World client software to provide the option to use a plaintext TCP relay for SEEJobs between the hardserver and the CodeSafe 5 application instead of an SSH tunnel. This is an opt-in feature, and the SSH tunnel continues to be used by default.

Use of the plaintext relay enables optimization of the latency and throughput for SEEJobs communication for scenarios where this is compatible with the threat model.

The plaintext relay is available in the following two scenarios: * When the CodeSafe 5 appli-

cation is loaded directly from the nShield 5c appliance, as described in CodeSafe 5: Auto-load from 5c (Connect) config and multi-client multiplexing of SEEJobs (NSE-71048). In this case, there is plaintext communication internally within the appliance between the 5c (Connect) hardserver and the CodeSafe 5 application, but SEEJobs communication over the network between the remote client hardserver and the 5c is secured with nCipher Secure Transport/Impath in the usual manner. * When loading a CodeSafe 5 application on a local 5s (Solo form factor), where the traffic is not going over an external network.

The plaintext relay cannot be configured from a remote client `[codesafe]` configuration to communicate directly over the network to a 5c (Connect form factor) HSM and attempts to do so will be refused as such a configuration would not be secure.

The plaintext relay for SEEJobs can be enabled by specifying `seejobs_transport=plain` in the `[codesafe]` section of the nShield 5c config file or client-side config file for communication with an nShield 5s. If not set, it will implicitly be equivalent to the default of `seejobs_transport=ssh` and the SSH tunnel will continue to be used.

3.5. CodeSafe 5: C++ 17 support (NSE-77086)

Security World v13.9 STS Release 3 formalizes support for CodeSafe 5 with C\++17.

The C++ compiler for CodeSafe 5 was previously shipped as part of the CodeSafe SDK, but the SDK did not define the build flags nor provide examples for building with C\++ 17.

The `helloplus` example has been added (`/opt/nfast/c/csd5/examples/netsee/helloplus` on Linux and `C:\Program Files\nCipher\nfast\c\csd5\examples\netsee\helloplus` on Windows) to show how to build a simple CodeSafe 5 application with C+17 and demonstrate various C\+ language and library features working with the cross-compiler.

If you are not using CMake to build your CodeSafe 5 application, consult the C\++ compiler and linker flags defined in the SDK's `codesafe-toolchain-nshield5-csee.cmake` file to obtain the correct flags for your build files.

Some header updates have also been made to improve support for C+: * The reserved C\+ keyword `export` was used as a field name in `M_Command.args.export` and `M_Reply.reply.export`. This affected applications using headers that pulled in the nCore types, such as `nfastapp.h` or `seelib.h`. By default, the field will now be renamed using the preprocessor to `exportcmd` when compiling with a C++ compiler. If an application has already worked around this issue by defining `export` before including relevant headers, the preprocessor renaming will not be applied, and the user's existing work-around will continue to behave as before. If `STDMARSHAL_KEEP_EXPORT_RENAME` is defined before including relevant headers, `export` will not be `#undef`-ed after the affected headers, so that code can still refer

ence `M_Command.args.export` and `M_Reply.reply.export` for compatibility with C; this should only be done if `export` is not otherwise being used in the codebase. To completely disable these workarounds, define the `STDMARSHAL_NO_EXPORT_RENAME` macro before including relevant headers. * `seelib.h` now correctly defines `extern "C"` guards to allow it to be included in C\++ code.

3.6. CodeSafe 5: SDK improvements (NSE-74771)

Security World v13.9 STS Release 3 resolves the following issues in CodeSafe 5:

- Re-adding missing `NF_Copy_*` functions (for deep-copying nCore objects) to `seelib.a`
- Error handling changes for SEEJob processing
- Various defect fixes

Refer to Known and fixed issues for more information on fixed CodeSafe 5 issues in Security World v13.9 STS Release 3.

3.7. FIPS 205 SLH-DSA support added to the nShield PKCS #11 API (NSE-64745)

Security World v13.9 STS Release 3 introduces support for generating SLH-DSA keys using `CKM_SLH_DSA_KEY_PAIR_GEN`, with the following set of mechanisms available for sign and verify operations:

- `CKM_SLH_DSA`
- `CKM_HASH_SLH_DSA`
- `CKM_HASH_SLH_DSA_SHA256`
- `CKM_HASH_SLH_DSA_SHA512`
- `CKM_HASH_SLH_DSA_SHAKE128`
- `CKM_HASH_SLH_DSA_SHAKE256`

All twelve parameter sets, as defined within FIPS 205, are supported:

- `CKP_SLH_DSA_SHA2_128S`
- `CKP_SLH_DSA_SHAKE_128S`
- `CKP_SLH_DSA_SHA2_128F`
- `CKP_SLH_DSA_SHAKE_128F`
- `CKP_SLH_DSA_SHA2_192S`
- `CKP_SLH_DSA_SHAKE_192S`

- CKP_SLH_DSA_SHA2_192F
- CKP_SLH_DSA_SHAKE_192F
- CKP_SLH_DSA_SHA2_256S
- CKP_SLH_DSA_SHAKE_256S
- CKP_SLH_DSA_SHA2_256F
- CKP_SLH_DSA_SHAKE_256F

Use of these mechanisms requires a firmware version of v13.8 or greater and the PostQuantum feature to be enabled, see the *User Guide* for your HSM for more information.

See the *nShield PKCS #11 API Reference Guide* for further information on these mechanisms.

3.8. Java 25 support (NSE-73374)

The nCipherKM JCA/JCE Provider now supports Java 25 (both Oracle JDK and OpenJDK).

The following versions are supported:

- Java 17
- Java 21
- Java 25

3.9. DeriveMech_NISTKDFmGeneric support in JCE API (NSE-66713)

Security World v13.9 STS Release 3 introduces the Generic NIST KDF derive mechanism and makes it available as a JCE KDF, supporting all SHA-2 HMAC mechanisms as the PRF. The kx parameter is not currently supported.

3.10. MLDSA external mu use/support in PKCS#11 (NSE-73430)

Security World v13.9 STS Release 3 introduces support to PKCS#11 for CKM_ML_DSA_EXTERNAL_MU allowing for ML-DSA signing and verification by supplying an externally computed μ (mu) value instead of the full message as per FIPS-204.

3.11. AES-GCM Encryption in PKCS11 v2.40 with fips-140-level-3 mode Security World (NSE-71833)

Security World v13.9 STS Release 3 introduces encryption with CKM_AES_GCM which now accepts an IV of zero length. If this is supplied, a 12-byte IV will be generated by the module and prepended to the ciphertext. Decryption still requires an IV. CKM_AES_GCM encryption with a zero length IV is permitted in a FIPS level 3 enforced Security World.

3.12. FIPS-204 ML-DSA in CNG (NSE-64737)

Security World v13.9 STS Release 3 introduces Microsoft CNG support for the ML-DSA pure and pre-hash signing algorithms.

3.13. FIPS-205 SLH-DSA signature scheme in CNG

Security World v13.9 STS Release 3 introduces Microsoft CNG support for the SLH-DSA pure and pre-hash signing algorithms.

3.14. Open Source Software Updates in the Security World v13.9 STS Release 3

The following Open Source components have been updated as part of Security World v13.9 STS Release 3:

3.14.1. CodeSafe 5

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
musl	1.1.24	1.2.5

3.14.2. Security World Software

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
Go	1.24.9	1.25.7
golang.org/x/crypto	v0.43.0	v0.48.0
golang.org/x/sys	v0.37.0	v0.41.0

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
OpenSSL	3.0.18	3.0.19
Python	3.11.14	3.11.15
SQLite	3.50.3	3.51.3

3.14.3. Security World Software Python Packages

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
filelock	3.13.1	3.25.2
libpng	1.6.37	1.6.54
pip	24.0	25.3
urllib3	2.5.0	2.6.3
wheel	0.45.1	0.46.3

3.14.4. nShield Connect XC and nShield 5c

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
e2fsprogs	1.46.5	1.47.3
libglib2	2.82.5	2.87.2
libopenssl	3.0.18	3.0.19
openssl	3.0.18	3.0.19
python	3.11.14	3.11.15
sqlite	3.50.3	3.51.3
util-linux	2.38	2.41.3

3.14.5. Remote Administration Client

OSS Name	v13.9 STS Release 2	v13.9 STS Release 3
libpng	1.6.37	1.6.54
Python	3.11.14	3.11.15
urllib3	2.5.0	2.6.3

4. Deprecated and discontinued features

The following features are deprecated or discontinued in Security World v13.9. If you have been using these features, plan for a new configuration and workflow that does not make use of the feature:

- KeySafe
  This is the legacy Java application. **KeySafe 5** continues to be supported in v13.9. KeySafe information has been removed from the user documentation for v13.9 and later releases. Previous user documentation releases that cover KeySafe continue to be available at https://nshielddocs.entrust.com/.

5. Firmware images

5.1. nShield 5s firmware

The nShield 5s HSM firmware consists of 3 major components:

- Primary Image
- Recovery Image
- Bootloader

The firmware for Security World v13.9 STS Release 3 only updates the Primary image. The Recovery image and Bootloader can be kept at previously released versions.

Details on what the components are used for and how to upgrade the different components are detailed in Upgrade nShield 5s HSM Firmware. Read this section prior to upgrading any nShield 5s.

5.1.1. nShield 5s firmware

Security World v13.9 STS Release 3 does not ship an updated nShield 5s firmware. The shipped firmware for the nShield 5s is from Security v13.9 STS Release 2.

Type	Version	Description	Directory	VSN
Latest	13.8.4	Firmware with features from the v13.9 STS Release 2.	`firmware/nShield5s/latest/nShield5s-13.8.4-vsn5.npkg`	5

5.2. Solo XC firmware

Security World v13.9 STS Release 3 does not ship an updated Solo XC firmware. The shipped firmware for the Solo XC is from Security v13.9 STS Release 2.

Type	Version	Description	Directory	VSN
Latest	13.8.3	Firmware with features from the v13.9 STS Release 2.	`firmware/SoloXC/latest/soloxc-13.8.3-vsn37.nff`	37

5.3. nShield Edge Firmware

There is no updated nShield Edge firmware being made available with the v13.9 release.

6. Connect images

The nShield firmware and Connect Image ISO includes v13.9.5 Connect images that contain the Solo XC and nShield 5s firmware described in Firmware images.

6.1. Install a Connect image

As part of the Security World installation, the `/opt/nfast/nethsm-firmware` directory is created, but it is empty. When the Connect image that needs to be installed has been chosen, the subdirectory and the image should be copied from the nShield firmware and Connect ISO into the `/opt/nfast/nethsm-firmware` directory and installed onto the Connect as usual.

6.2. nShield 5c images

Type	Version	Description	Firmware included	Directory	VSN
Latest	13.9.5	13.9 nShield 5c image with the v13.9 STS Release 2 nShield 5s 13.8 firmware	13.8.4	`nethsm-firmware/latest-all-13.9.5-vsn33/`	33

For security reasons the Version Security Number (VSN) of the nShield 5c image has been increased to 33. Upon updating to the new images it will **not** be possible to downgrade to previous releases.

The following releases **can** be updated to post this change:

- v13.6.12 LTS Update 4
- v13.6.14 LTS Update 5
- v13.6.15 LTS Update 6

6.3. Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
Latest	13.9.5	13.9 Connect XC image with the v13.9 STS Release 2 Solo XC 13.8 firmware	13.8.3	`nethsm-firmware/latest-all-13.9.5-vsn33/`	33

For security reasons the Version Security Number (VSN) of the nShield

> Connect XC image has been increased to 33. Upon updating to the new images it will **not** be possible to downgrade to previous releases.
>
> The following releases **can** be updated to post this change:
>
> - v13.6.12 LTS Update 4
> - v13.6.14 LTS Update 5
> - v13.6.15 LTS Update 6

7. Upgrade from previous releases

7.1. Install 13.9.5 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.

7.2. 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 intermedi ate 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 configura tion is not compatible (either through current version or after upgrading to a newer version of the firmware). Please contact nshield.sup-port@entrust.com if you experience any issues following an upgrade or during integration activity.

7.3. Upgrade nShield 5s HSM Firmware

As detailed in the *nShield v13.9.5 HSM User Guide*, the nShield 5s HSM firmware consists of 3 major components:

- Primary Image
- Recovery Image
- Bootloader

During normal operation, the nShield 5s is running firmware that is loaded from the Primary image. If required, the nShield 5s can be forced into recovery mode to run firmware loaded from the Recovery image. The main purpose of recovery mode is to allow essential maintenance activities that are not possible when the nShield 5s is running the primary image firmware.

7.3.1. nShield 5s Firmware Version Check

Following the upgrade, the nShield 5s primary image, recovery image and bootloader versions can be checked using the `hsmadmin` command:

```
hsmadmin status --json
```

As an example, following an upgrade, it should report as follows:

```
"mode": "primary",
"primary-version": "13.8.4-0-97cca219",
"recovery-version": "13.5.0-0-e2ec16eefd",
"uboot-version": "1.4.1-0-edb84d6e",
```

7.3.2. Upgrading the nShield 5s Primary & Recovery Image

Upgrade packages may contain updates for any of these components. The same upgrade method is used in all cases. The system will automatically detect which components are included in the update package and will load the firmware to the correct location.

It is not recommended to upgrade both the Primary and Recovery images at the same time. The recommended procedure is to upgrade the Primary firmware first. Test that the system performs as expected and then upgrade the Recovery firmware at a later date.

The primary and recovery images can be upgraded using the following command:

For primary:

```
hsmadmin upgrade nShield5s-13.8.4-vsn5.npkg --esn module-esn
```

and for recovery:

```
hsmadmin upgrade nshield5s-recovery-13-5-0.npkg --esn module-esn
```

7.3.3. Upgrading the nShield 5s Bootloader

The bootloader is the program that boots the HSM and loads the main application. The nShield 5s has a discrete bootloader that can be updated independently of the Primary and Recovery images.

7.3.3.1. Pre-Requisites

Whilst the bootloader is an independent part of the firmware, the capability to upgrade the bootloader on the nShield 5s was introduced as part of the Security World v13.4 firmware release. For earlier versions of firmware prior to v13.4, the nShield 5s firmware must be upgraded to v13.4 as a minimum to enable this bootloader upgrade to work. Contact nShield Support for details of obtaining the v13.4 version of firmware.

7.3.3.2. Upgrading bootloader

Once the primary firmware is at version v13.4 or later, the bootloader can be upgraded using the same hsmadmin upgrade command:

```
hsmadmin upgrade nShield5s-uboot-1-4-1.npkg --esn module-esn
```

Note: Once the bootloader version is upgraded, it is not possible to downgrade the bootloader to the previous version. The Primary and Recovery images can still be downgraded and upgraded independent of this bootloader version.

7.4. Upgrade a Connect XC image

If the 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 Connect image and needs to be first upgraded to an intermediate version. Any of the Connect image versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of Connect image.

8. Compatibility

8.1. Supported hardware

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

- nShield 5s (Base, Mid, High)
- Solo XC (Base, Mid, High)
- nShield 5c (Base, Mid, High)
- Connect XC (Base, Mid, High, Serial Console)

8.2. Supported operating systems

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

Operating System	Solo XC	nShield 5s	Connect XC, nShield 5c
Microsoft Windows 10 x64	Y	Y	Y
Microsoft Windows 11 x64	Y	Y	Y
Microsoft Windows Server 2019 x64	Y	Y	Y
Microsoft Windows Server 2022 x64	Y	Y	Y
Microsoft Windows Server 2022 Core x64	Y	Y	Y
Microsoft Windows Server 2025 x64	Y	Y	Y
Red Hat Enterprise Linux 8 x64	Y	Y	Y
Red Hat Enterprise Linux 9 x64	Y	Y	Y
SUSE Enterprise Linux 15 x64	Y	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y	Y
Oracle Enterprise Linux 9 x64	Y	Y	Y

Security World v13.9.5 support is restricted to the x64 architecture. Additional mainstream x64-based Linux distributions other than those listed above may be compatible, however Entrust cannot guarantee this compatibility.

8.3. API support

8.3.1. Java

The versions in the table below are for both Oracle JDK and Open JDK.

Version	Supported
17	Y
21	Y
25	Y

8.3.2. Python

This lists the versions of Python that are supported.

Version	Supported
3.11	Y

8.4. Supported hypervisors and virtual environments

Operating System	Solo XC	nShield 5s	Connect XC, nShield 5c
Microsoft Hyper-V Server 2016	Y	Y	Y
Microsoft Hyper-V Server 2019	Y	Y	Y
Microsoft Hyper-V Server 2022	Y	Y	Y
VMWare ESXi 7.0	Y	N	Y
VMWare ESXi 8.0	Y	Y	Y
Citrix XenServer 8.2	Y	N	Y

8.5. Supported compilers for Microsoft Windows C developers

Security World v13.9.5 C libraries for Windows were built using Visual Studio 2022 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 2022.

Version	Supported
2022	Y

9. Known and fixed issues

Reference	Scope	Status	Description
NSE-76421	Connect	Resolved	Addressed an issue where the Connect unit failed to respond correctly to Path MTU Discovery (PMTUD). **Resolved** in 13.9 Connect images.
NSE-76078	Connect	Resolved	Addressed an issue where the `getservlog` ApplianceCommand no longer functioned on Connect/5c units for log fetching. **Resolved** in 13.9 Connect images.
NSE-75862	Client-side	Resolved	Addressed an issue where `C_Decapsulate` and `C_Encapsulate` did not support `CKA_TOKEN=True`. **Resolved** in 13.9 client-side.
NSE-75763	Client-side	Resolved	Addressed an issue where the NFKM engine would silently fail if using a stale preload file. **Resolved** in 13.9 client-side.
NSE-75671	Client-side	Resolved	Removed the `pkcs11req` appname from `generatekey`. **Resolved** in 13.9 client-side.
NSE-75628	Client-side	Resolved	Addressed an issue with the help output for the `nethsmadmin` utility. **Resolved** in 13.9 client-side.
NSE-75038	Client-side	Resolved	Addressed an issue where calling C_GenerateKey before C_Initialize would return CKR_ARGUMENTS_BAD. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-75037	Client-side	Resolved	Addressed an issue where calling functions would segfault if called before C_Initialize. **Resolved** in 13.9 client-side.
NSE-75400	Client-side	Resolved	Addressed an issue where pkcs11extra.h erroneously referenced ML-DSA mechanisms after the 3.2 header adoption. **Resolved** in 13.9 client-side.
NSE-74960	Client-side	Resolved	Addressed an issue where `ulMinKeySize` and `ulMaxKeySize` were incorrect for multiple PKCS#11 mechanisms. **Resolved** in 13.9 client-side.
NSE-74499	Client-side	Resolved	Addressed an issue where `ckinfo` and `ckcheckinst` would return the wrong header version. **Resolved** in 13.9 client-side.
NSE-74156	Client-side	Resolved	Addressed an issue where an assertion would occur when calling `perfcheck --diff` under certain circumstances. **Resolved** in 13.9 client-side.
NSE-74125	Client-side	Resolved	The slotinfo for loadshared slots now includes the `CKF_HW_SLOT` flag. Softcard slots may be distinguished from OCS slots by the `CKF_REMOVABLE_DEVICE` flag. **Resolved** in 13.9 client-side.
NSE-74083	Client-side	Resolved	Addressed an issue where Java PublishedSEEWorld's getInitStatus() method would throw a null pointer exception for already successfully initialized Worlds. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-74078	Client-side	Resolved	Removed the `embed` key type from `generatekey`. **Resolved** in 13.9 client-side.
NSE-73821	Connect	Resolved	Refined the `appliance-cli` help output. **Resolved** in 13.9 Connect images.
NSE-73585	Client-side	Resolved	Refined the error reporting for `cfg_remoteslots` when the importing module is a remote module. **Resolved** in 13.9 client-side.
NSE-72542	Client-side	Resolved	Addressed an issue where SEElib_StartProcessorThreads() no longer crashes if nthreads is too high. **Resolved** in 13.9 client-side.
NSE-72539	Client-side	Resolved	Addressed an issue where 'pending job table full' / Status_ObjectNotReady error from SEElib_Transact() no longer occurs when many hundreds of threads are created. **Resolved** in 13.9 client-side.
NSE-72508	Client-side	Resolved	Addressed an issue where a CodeSafe 5 application would crash if C++ threads are used. This was due to the CMake build flags defined in the SDK not including the required flags for correct and consistent C++ builds. If not using CMake to build your CodeSafe 5 application, the C\++ compiler and linker flags defined in the SDK's `codesafe-toolchain-nshield5-csee.cmake` file should be consulted to obtain the correct flags for your own build files. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-72389	Client-side	Resolved	Addressed an issue where a `Failed to add a watch for /run/user/0/systemd/ask-password: Permission denied` warning would be displayed during installation of the product, or during the hardserver start/stop process on Red Hat Enterprise Linux 10 x64. **Resolved** in 13.9 client-side.
NSE-72241	Client-side	Resolved	Addressed an issue where objects could leak in the Java CoreKey class. **Resolved** in 13.9 client-side.
NSE-72090	Connect 5c	Resolved	Addressed an issue where new remote client connections to a Connect or 5c would be rejected if the module failed after startup (this did not affect clients that were already connected when the failure occurred). This change supports remote recovery using a privileged client, using "nethsmadmin -r -m1" to reboot the appliance, or (in the case of 5c) using "nopclear-fail -r -m1" to attempt to retry after an error (e.g. to clear an SOS code). Note that if an error is cleared without a reboot, it may be necessary to restart the client hardserver (or remove and re-import the 5c using nethsmenroll) in order to reflect the updated state of no longer being Failed. This is not required if the appliance is rebooted instead. **Resolved** in 13.9 client-side.
NSE-71960	Client-side	Resolved	Addressed an issue where 'cnglist --show-sd' would not produce extra information correctly. **Resolved** in 13.9 client-side.
NSE-71959	Client-side	Resolved	Addressed an issue where NTE_NOT_FOUND errors would appear when listing CNG keys verbosely. **Resolved** in 13.9 client-side.
NSE-71927	Client-side	Resolved	Addressed an issue where csadmin image signing can fail when not all modules are usable within the current Security World. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-71923	Client-side	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 client-side.
NSE-71913	Client-side	Resolved	Addressed an issue where spurious errors would appear in the CodeSafe 5 logfile from SEEJob processing. **Resolved** in 13.9 client-side.
NSE-71851	Client-side	Resolved	`csadmin` image signing subcommands now support specifying the application type (such as 'simple' or 'seeinteg') for Developer ID keys and Application Signing Keys. The previous default of 'simple' application type is retained for now for compatibility, but 'seeinteg' may be a more convenient choice for the Application Signing Key in order to support the use of the 'seeintegname' option in the 'generatekey' tool to generate keys that are restricted to the CodeSafe application. **Resolved** in 13.9 client-side.
NSE-71838	Client-side	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 client-side.
NSE-71732	Client-side	Resolved	Fixed an issue where the automatic configuration of CodeSafe 5 via [codesafe] config section or the hsc_codesafe tool directly failed to stop existing applications on v13.4 firmware. [codesafe] configuration section and hsc_codesafe tool are now supported with v13.4 firmware when using the latest SecWorld and CodeSafe SDK. **Resolved** in 13.9 client-side.
NSE-71688	Documentation	Resolved	The Security Manual has been updated to state the limitations of the Connect/5c tamper log, and to emphasize the recommendation that Audit Logging should be enabled in new Security World creation as the primary security log mechanism. **Resolved** in 13.9 documentation.

Reference	Scope	Status	Description
NSE-71681	Firmware (5s only)	Resolved	Addressed an issue where a zero length salt could cause the HSM to fail. **Resolved** in 13.8.1 firmware.
NSE-71638	Documentation	Resolved	Updated the Security Manual to clarify the HSM form factors and the distinction between the Connect/5c appliance and the certified HSM inside it. **Resolved** in 13.9 documentation.
NSE-71637	Documentation	Resolved	Updated the Security Manual to clarify HSM decommissioning steps, especially that factory state is recommended for Connect/5c/5s modules, not just erasure of the Security World. **Resolved** in 13.9 documentation.
NSE-71635	Connect XC and 5c	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 Connect Images.
NSE-71617	Connect XC and 5c	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 Connect Images.
NSE-71565	Connect XC and 5c	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 Connect Images.
NSE-71493	Client-side	Resolved	Addressed an issue where _nfpython3.so in the CodeSafe 5 SDK was not stripped of debug symbols, increasing the CodeSafe 5 container size. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-71350	Connect	Resolved	Addressed an issue where the Connect unit cannot upgrade from v12.x Connect images. **Resolved** in 13.9 Connect images.
NSE-71308	Connect	Resolved	Fixed an issue where client licenses for 4 clients would not be applied correctly on Connect XC/5c in v13.6 or v13.7 Connect images. This issue is fixed in v13.6.12 (latest v13.6 LTS) and in v13.9 Connect images. **Resolved** in 13.9 Connect images.
NSE-71089	Firmware	Resolved	Addressed an issue to stop accepting elliptic curve domain parameters with certain types of unsupported fields. **Resolved** in 13.8 firmware.
NSE-70765	Client-side	Resolved	Addressed an issue where `ncperftest` would not work with pre-created keys. **Resolved** in 13.9 client-side.
NSE-70686	Client-side	Resolved	Addressed an issue where the nShield 5s wouldn't be available for several minutes after a reboot. **Resolved** in 13.9 client-side.
NSE-70540	Firmware	Resolved	Addressed an issue where launcher does not check certificate policies for CS5 intermediate certs. **Resolved** in 13.8 firmware.
NSE-70375	Firmware (5s only)	Resolved	Addressed an issue with EllipticCurve ASN.1 inputs **Resolved** in 13.8.1 firmware.
NSE-70302	Client-side	Resolved	Addressed an issue where `cksotool` doesn't ask for FIPS auth in a sensible way. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-70283	Client-side	Resolved	Addressed an issue where 'signextra' with non-FIPS mechanisms gives StrictFIPS140 error on load. **Resolved** in 13.9 client-side.
NSE-70232	Firmware (5s only)	Open	While under a prolonged period of heavy load generated by continuous signing or key generation operations using MLDSA 44, the 5s or 5c unit may fail with a `RC_SP_WRONG_PREAMBLE` error in the logs. Restarting the unit will restore it to a working state. **Issue first found** in 13.8.1 firmware
NSE-70194	Client-side	Resolved	Addressed an issue where harmless operations are not logged if a key has any restrictions. **Resolved** in 13.9 client-side.
NSE-70105	Client-side	Resolved	Addressed an issue where the CodeSafe XC NFKM libraries for GLIBC were missing from the CodeSafe installer. **Resolved** in 13.9 client-side.
NSE-70062	Client-side	Resolved	Fixed an issue where a CodeSafe 5 application would abort if more than 154 jobs were enqueued simultaneously. **Resolved** in 13.9 client-side.
NSE-70007	Firmware	Resolved	Addressed an issue where KCDSA domain validation did not check parameters correctly. **Resolved** in 13.8 firmware.
NSE-69976	Client-side	Resolved	Addressed an issue where generatekey was missing AES import. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-69881	Client-side	Resolved	Addressed an issue where various PKCS11 functions were not thread-safe. **Resolved** in 13.9 client-side.
NSE-69925	Client-side	Resolved	Addressed various memory leaks in RQCard library. **Resolved** in 13.9 client-side.
NSE-69830	Client-side	Resolved	Addressed an issue where ch_checkkey() didn't reject non-FIPS keys in FIPS mode. **Resolved** in 13.9 client-side.
NSE-69623	Firmware	Resolved	Addressed RSA length inconsistencies. **Resolved** in 13.8 firmware.
NSE-69523	Client-side	Resolved	Addressed small memory leaks in C_Initialize, when run against a FIPS level 3 enforced Security World. **Resolved** in 13.9 client-side.
NSE-69520	Client-side	Resolved	Fixed an issue on Windows where perfcheck called the deprecated Windows wmic tool, which may no longer be installed, to query CPU information for its report. **Resolved** in 13.7 client-side.
NSE-69503	Client-side	Resolved	Addressed an issue where the signers_transact() was broken in CodeSafe 5 Developer examples. **Resolved** in 13.9 client-side.
NSE-69326	Client-side	Resolved	Addressed an issue where sendcerts permits groups below the ciphersuite's minimum. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-69076	Client-side	Resolved	Improved the CodeSafe 5 crash reporter so that some information would be provided even when a full backtrace was not available. **Resolved** in 13.7 client-side.
NSE-69053	Client-side	Resolved	Addressed an issue where the nShield 5s driver failed to report the version in dmesg. **Resolved** in 13.9 client-side.
NSE-69048	Client-side	Resolved	Added missing `NF_Copy_*` functions (for deep-copying nCore objects) to `seelib.a` for CodeSafe 5. **Resolved** in 13.9 client-side.
NSE-69020	Connect	Resolved	Addressed an issue where the Connect 5c upgrade will fail to upgrade if the time is not set on the module. Refer to Unset module RTC upgrade issue on Connect 5c units for more information. **Resolved** in 13.9 Connect images.
NSE-68919	Client-side	Resolved	The csadmin tool is now strict by default in requiring that the "launcher" service on the HSM has an attestation certificate. This certificate is only available in v13.5 and later firmware (and a factory state may be required to generate it if it is not present). If using a firmware version without support for attestation certificates (such as v13.4), the NC_SSH_ATTEST_CERT or NC_SSH_ATTEST_<esn> environment variables can be set in the environment of the csadmin tool to control the behaviour if there is a missing certificate. It can be set to IGNORE (connection proceeds silently), WARN (previous behavior prior to this change), or FAIL (connection will fail, new behavior). Setting NC_SSH_ATTEST_CERT=WARN or NC_SSH_ATTEST_CERT=IGNORE is suggested if using v13.4 firmware. It is recommended that factory state be done if necessary to generate the certificate if using v13.5 or later firmware if it is currently absent. **Resolved** in 13.9 client-side.
NSE-68682	Client-side	Resolved	Addressed an issue where `nethsmadmin --list-images` would return the wrong error message if the RFS IP was not specified. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-68675	Client-side	Resolved	Addressed some performance and scheduling issues. **Resolved** in 13.9 client-side.
NSE-68534	Firmware	Resolved	Addressed an issue where legacy key-migration mistakes could lead to an inability to carry out further key-migration. **Resolved** in 13.8 firmware.
NSE-68179	Client-side	Resolved	Fixed an issue on Windows where an unwanted message box could appear relating to the TVD driver installation during a Security World software or Remote Administration software installation. **Resolved** in 13.7 client-side.
NSE-68093	Firmware	Resolved	Addressed performance issues with CodeSafe 5 administration operations. **Resolved** in 13.8 firmware.
NSE-68044	Client-side	Resolved	Addressed an issue where the csadmin utility failed to include the scope ID when reporting link-local addresses. **Resolved** in 13.7 client-side.
NSE-68007	Client-side	Resolved	Fixed an issue where incorrect parameters in client nCore commands (like wrong module number) were unnecessarily reported as errors in the hardserver log. **Resolved** in 13.7 client-side.
NSE-67930	Client-side	Resolved	Fixed an issue where CodeSafe 5 CSEE (SEElib) applications could fail with SIGPIPE in some cases. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-67913	Firmware	Resolved	Addressed an issue with service restrictions and permissions. **Resolved** in 13.8 firmware.
NSE-67846	Client-side	Resolved	Fixed an issue where the nShield Audit Service could fail to correctly resume handling the export and expiry of system logs where an interruption had occurred during export on a previous run. **Resolved** in 13.7 client-side.
NSE-67839	Client-side	Resolved	Addressed an issue where DHPrivate 'xlength' checking is not exact. **Resolved** in 13.9 client-side.
NSE-67776	Firmware	Resolved	Addressed an issue where the `ch_generatekeypair` didn't always spot bogus key generation parameters. **Resolved** in 13.8 firmware.
NSE-67758	Firmware	Resolved	Addressed an issue where the firmware would provide incomplete validation error messages in response to the `csadmin` utility loading a CodeSafe 5 application. **Resolved** in 13.8 firmware.
NSE-67601	Firmware	Resolved	Addressed an issue where the incorrect BIOS code would be reported when the VCM would fail to start in single-tenant mode. **Resolved** in 13.7 firmware.
NSE-67579	Client-side	Resolved	Fixed an issue where output from nshieldaudit when printing to stdout rather than to file was not in JSON format as intended. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-67248	Client-side	Resolved	Addressed an issue where the auditlog spooler service would log every 5 minutes when unconfigured. **Resolved** in 13.9 client-side.
NSE-66905	Documenta-tion	Resolved	The documented set of allowed CodeSafe 5 system calls now reflects the set of system calls allowed by seccomp. **Resolved** in 13.7 documentation.
NSE-66800	Client-side	Resolved	Addressed an issue where some client-side CodeSafe developer libraries were shipped as source code rather than built as libraries. **Resolved** in 13.9 client-side.
NSE-66437	Connect	Resolved	Made the Connect CLI command `setminvsn` more user-friendly. **Resolved** in 13.7 Connect images.
NSE-66432	Connect	Resolved	Addressed an issue with `hsmdiagnose` where a test was incorrectly skipped. **Resolved** in 13.7 Connect images.
NSE-66415		Open	The appliance-cli gethsmstatus command returns a 'Failed to retrieve status' error when executed against Legacy FIPS Con-nect image. This means the version information for the Legacy FIPS Connect image cannot be retrieved at this time. **Issue first found** in 13.6
NSE-66256	Client-side	Resolved	Addressed an issue where the message "Failed to parse last log data from current log" would be displayed in the nshieldau-ditd logfile. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-66232	Firmware	Resolved	Addressed a firmware issue which prevented CodeSafe 5 applications built with 13.4 SDK from working on later versions of firmware. Applications built with 13.4 SDK will work on 13.7 and later firmware, but they cannot run on 13.5 firmware which does not have this fix. **Resolved** in 13.7 firmware.
NSE-65799	Client-side	Resolved	Addressed an issue where a stack trace would be displayed during installation on SLES12 platforms. **Resolved** in 13.7 client-side.
NSE-65310	Client-side	Resolved	Addressed an issue where encryption with CKM_AES_CTR in PKCS#11 failed if used with a token key that had not been loaded on the module. **Resolved** in 13.9 client-side.
NSE-65292	Firmware	Resolved	Addressed an issue where a Status_Failed message would occur instead of Status_DecryptFailed with RSAUnwrap and AES Key unwrapping under certain circumstances. **Resolved** in 13.7 firmware.
NSE-65229	Firmware	Resolved	Addressed an issue where DeriveMech_PublicFromPrivate doesn't work with Ed448Private. **Resolved** in 13.7 firmware.
NSE-65109	Firmware	Resolved	Addressed an issue where the Solo XC was too enthusiastic to clear the module from the clear button. **Resolved** in 13.7 firmware.
NSE-64992	Client-side	Resolved	Addressed an issue where the `ncperftest` utility could crash if an unreasonable queue size is set. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-64885	Client-side	Resolved	Addressed an issue where the CONNECTION ERROR: Unable to connect to 'monitor' failure would occur when multiple clients were attempting to connect to the monitor service. **Resolved** in 13.7 client-side.
NSE-64592	Documentation	Resolved	Addressed an issue where the M_AESmGCM HTML docs omitted the ciphertext format. **Resolved** in 13.7 documentation.
NSE-64625	Client-side	Resolved	Addressed an issue where HSM Pool Mode would not work in PKCS #11 with a v13 client-side and older v12 firmwares. **Resolved** in 13.9 client-side.
NSE-64570	Client-side	Resolved	`nfkmattest` will now display the filename if a problem is encountered when reading the file. **Resolved** in 13.9 client-side.
NSE-64525	Client-side	Resolved	Addressed an issue where nfkmverify didn't accept keys which could perform ECIES unwrapping. **Resolved** in 13.9 client-side.
NSE-64438	Firmware	Resolved	Addressed an NVMWearLevel issue for Solo XC and nShield 5s units. **Resolved** in 13.7 firmware.
NSE-64409	Client-side	Resolved	Fixed an issue which prevented later CodeSafe SDKs from running on v13.4 firmware. Rebuilding application with the latest CodeSafe SDK will enable it to run on v13.4 firmware. This re-enables support for applications written in C. For Python support, the v13.4 CodeSafe SDK must continue to be used with v13.4 firmware. Newer CodeSafe SDK is supported on v13.5 and later firmware in all cases. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-64304	Client-side	Resolved	Addressed an issue where D3S certificates appear in ncoreapi's stderr. **Resolved** in 13.9 client-side.
NSE-63892	Client-side	Resolved	Addressed an issue where generated nCore HTML pages could be missing. **Resolved** in 13.7 client-side.
NSE-63502		Open	When using KeySafe5 with the agent on the Connect the following error will populate the logs 'Command failed: monitor codesafestats get-all'. Users should increase the codesafe_update_interval using the ks5agent command via the Connect CLI. ks5agent cfg codesafe_update_interval=48h If you wish the logs to be cleared then enabling the Audit tooling will expire the system logs containing the above error. **Issue first found** in 13.6
NSE-63449	Client-side	Resolved	Addressed an issue in PKCS#11 where the following error would be reported: 'Key generation certificate with no private/secret key?' **Resolved** in 13.7 client-side.
NSE-63444	Client-side	Resolved	Addressed an issue in PKCS#11 where confusion between nShield and PKCS#11 key type enum values could cause a 'NFBER_Encode_Octet_BitStr_Key failed for len' error. **Resolved** in 13.7 client-side.
NSE-63091	Client-side	Resolved	Fixed an issue where the C_GetAttributeValue return value could be overwritten. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-62984	Client-side	Resolved	Addressed an issue in `nethsmadmin` where the feature file help was misleading. **Resolved** in 13.9 client-side.
NSE-62533	Client-side	Resolved	Addressed an issue in PKCS#11 where SELinux would prevent CodeSafe 5 applications from binding on some ports. **Resolved** in 13.7 client-side.
NSE-62267	Client-side	Resolved	Addressed an issue where multiple hardware failures could occur on Edge units. **Resolved** in 13.9 client-side.
NSE-61967	Client-side	Resolved	Addressed an issue where the tar utility would be killed by seccomp when used within a CodeSafe 5 application. **Resolved** in 13.7 client-side.
NSE-61966	Client-side	Resolved	An issue has been fixed where, if a CodeSafe 5 application created files on its local disk, 'csadmin destroy' reported an error when trying to remove those files. **Resolved** in 13.9 client-side.
NSE-61540	Client-side	Resolved	Addressed an issue where the CS5 Compatibility Layer would not stay listening for incoming connections. **Resolved** in 13.7 client-side.
NSE-61148	Firmware	Resolved	Addressed an issue where the init log is not created by replacement Python code as it should be. **Resolved** in 13.7 firmware.
NSE-61033	Firmware (5s only)	Resolved	Addressed an issue where deprecated options were reported in the nShield 5s system logs. **Resolved** in 13.7 nShield 5s firmware.

Reference	Scope	Status	Description
NSE-60936	Firmware	Resolved	Addressed an issue where CodeSafe can lose trace data. **Resolved** in 13.7 firmware.
NSE-60779	Client-side	Resolved	Fixed an issue where the nShield 5c would fail to Factory State if the nShield 5s system log was full. **Resolved** in 13.9 Connect images.
NSE-60554	Client-side	Resolved	Addressed an issue where TUAK and Milenage session key generation performance had decreased due to the need to generate key generation certificates at the point of key generation. This has been resolved by adding a new PKCS#11 environment variable: CKNFAST_SESSION_TO_TOKEN, this is enabled by default. The default behaviour is to generate session keys without Key Generation Certificates. This can be disabled by setting CKNFAST_SESSION_TO_TOKEN=0. **Resolved** in 13.7 client-side.
NSE-59598	Client-side	Resolved	Fixed an issue where RQCard used in conjunction with nflog could cause a segmentation fault. **Resolved** in 13.9 client-side.
NSE-59584	Client-side	Resolved	Addressed an issue where it wasn't possible to generate a CodeSafe 5 CSR using the `csadmin` utility on Windows systems if the OCS has a passphrase set. **Resolved** in 13.9 client-side.
NSE-59281	Client-side	Resolved	Addressed an issue where CodeSafe developer id certificates can be issued for RSA keys and the issued RSA keys can now sign images. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-57030	Client-side	Resolved	On Linux, the sshadmin client key for nShield 5s is now backed-up automatically to /root/.ssh/id_nshield5_sshadmin as a precaution against /opt/nfast/services/client directory being deleted. This backup is restricted to the local machine by default. It is recommended on both Windows and Linux to backup the sshadmin key if using nShield 5s. If it may be necessary to move the HSM to a different machine (or to reinstall the OS) at a later stage, the key should be backed up with the "hsmadmin keys backup --passphrase" option so that it is protected by a passphrase rather than being restricted to the local machine and OS installation. **Resolved** in 13.9 client-side.
NSE-55780		Open	Starting a CodeSafe 5 application on an nShield 5c produces the message "Could not find nshield network interfaces for service discovery" in the verbose output. **Issue first found** in 13.4
NSE-55428		Open	Building classic CodeSafe examples fails with older compiler. **Issue first found** in 13.4
NSE-55425	Firmware	Resolved	Addressed an issue where 'Unable to perform operation due to service interdependency lock' was reported when using the `csadmin` utility. **Resolved** in 13.7 firmware.
NSE-55378		Open	Minor inconsistency when enabling autostart via csadmin config.
NSE-55142		Open	From 13.4 keys generated using ckrsagen will now produce a warning using nfkmverify, this is due to stricter policy enforce on unwrap permissions. To overcome this use CKA_UNWRAP_TEMPLATE when generating PKCS#11 keys. **Issue first found** in 13.4

Reference	Scope	Status	Description
NSE-55136	Client-side	Resolved	Fixed an issue where offline produced CodeSafe 5 image signatures would fail CreateSEEConnection. **Resolved** in 13.9 client-side.
NSE-53090	Client-side	Resolved	Fixed an issue where using `nethsmadmin -f` provided the wrong path to use when applying features. **Resolved** in 13.9 client-side.
NSE-52456	Firmware (5s only)	Resolved	Addressed an issue where hsmadmin settime would leave the module around 2 seconds behind the host. **Resolved** in 13.7 nShield 5s firmware.
NSE-52302	Firmware (5s only)	Resolved	Addressed an issue with impath command sanitization. **Resolved** in 13.8.1 firmware.
NSE-50848	Client-side	Resolved	Fixed an issue where `ckmechinfo` would advertise wrap support that didn't work. **Resolved** in 13.9 client-side.
NSE-50050	Client-side	Resolved	Fixed an issue where the `nfkmverify` utility would not reject wrapping keys with the decrypt permission set. **Resolved** in 13.9 client-side.
NSE-49263	Client-side	Resolved	Fixed an issue where `mkaclx` printed an unclear error when a malformed ident string was specified on the command-line. **Resolved** in 13.9 client-side.
NSE-48991	Client-side	Resolved	Addressed an issue where nfkmutils.loadkey did not support softcards. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-43472	Client-side	Resolved	Addressed various issues with nfkmutils.loadkey. **Resolved** in 13.7 client-side.
NSE-42031	Firmware (XC only)	Resolved	Addressed a gradual increase in memory usage on nShield Solo XC modules. **Resolved** in 13.7 nShield Solo XC firmware.
NSE-41205	Firmware (XC only)	Resolved	An issue has been fixed that can cause a Solo XC or Connect XC HSM to enter an SOS state after many days of running. The issue would have generally manifested as an SOS-HV or SOS-HRTP, but other SOS codes are possible. A number of "SpiRe-tries" as reported by stattree utility may precede the failure. **Resolved** in 13.7 nShield Solo XC firmware.
NSE-48073		Open	Connect+ models running software earlier than v12 must first be upgraded to a v12 version before being upgraded to v13. See section Upgrade from previous releases for more details. **Issue first found** in 13.3
NSE-42017	Connect	Resolved	Fixed various issues with Connect XC and Connect 5c units. **Resolved** in 13.9 Connect images.
NSE-39031		Open	In Security World v12.10 a compliance mode was added to the Connect to allow compliance with USGv6 or IPv6 Ready requirements. **Issue first found** in 12.80
NSE-38156	Client-side	Resolved	Addressed an issue where Linux SNMP install depended on the `netstat` utility. This has now been replaced with the `ss` utility. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-36086	Client-side	Resolved	Addressed an issue where OpenSSH did not enable TCP_NODELAY resulting in latency spikes in CodeSafe 5 communication. **Resolved** in 13.7 client-side.
NSE-35974	Firmware	Resolved	Addressed an issue where `nvram-sw` could not delete all NVRAM files. **Resolved** in 13.8 firmware.
NSE-35520	Client-side	Resolved	Addressed an issue where the `nfkmverify` utility would reject future impath groups. **Resolved** in 13.9 client-side.
NSE-32255	Client-side	Resolved	Addressed an issue where the `ncperftest` help text omitted option to "test with an existing key". **Resolved** in 13.9 client-side.
NSE-28606		Open	Entrust 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 world then it is not possible to verify OCS and softcard protected keys directly with nfkmverify. The OCS or softcards must be preloaded prior to attempting to verify the keys.
NSE-26829	Client-side	Resolved	Addressed an issue where the reserved C++ keyword `export` was used as a field name in `M_Command.args.export` and `M_Reply.reply.export`. This affected applications using headers that pulled in the nCore types, such as `nfastapp.h` or `seelib.h`. By default, the field will now be renamed using the pre-processor to `exportcmd` when compiling with a C\++ compiler. **Resolved** in 13.9 client-side.
NSE-25401		Open	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. **Issue first found** in 12.60

Reference	Scope	Status	Description
NSE-24335		Open	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 **Issue first found** in 12.50
NSE-24026	Client-side	Resolved	Addressed an issue where the `nvram-sw` application read and write command did not require the `-n` option to function. **Resolved** in 13.9 client-side.
NSE-23982		Open	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. **Issue first found** in 12.50
NSE-23332	Client-side	Resolved	Addressed confusing help message when calling `rfs-setup --gang-client`. **Resolved** in 13.9 client-side.
NSE-22692	Client-side	Resolved	Addressed an issue where the `rocs` utility would truncate key names that were more than 24 characters long. **Resolved** in 13.9 client-side.
NSE-22484	Client-side	Resolved	Addressed an issue where the `generatekey` utility would ignore preloaded FIPS auth. **Resolved** in 13.9 client-side.

Reference	Scope	Status	Description
NSE-14406		Open	In the Connect config file the remote_sys_log config entry implies multiple entries can be defined but only one remote sys-log server can be configured. **Issue first found** in 12.50
NSE-8568	Client-side	Resolved	Addressed an issue on Linux platforms where the `edgeHandler.sh` script failed to cope with more than 1 serial_dtpp_device line in the configuration file. **Resolved** in 13.9 client-side.
NSE-7446	Client-side	Resolved	Addressed an issue where the PKCS#11 CMAC output length was wrong. **Resolved** in 13.9 client-side.
NSE-4551	Client-side	Resolved	Addressed an issue where unregistering the CNG providers using the `cngregister` utility would complain that it failed to delete the local machine key. **Resolved** in 13.9 client-side.