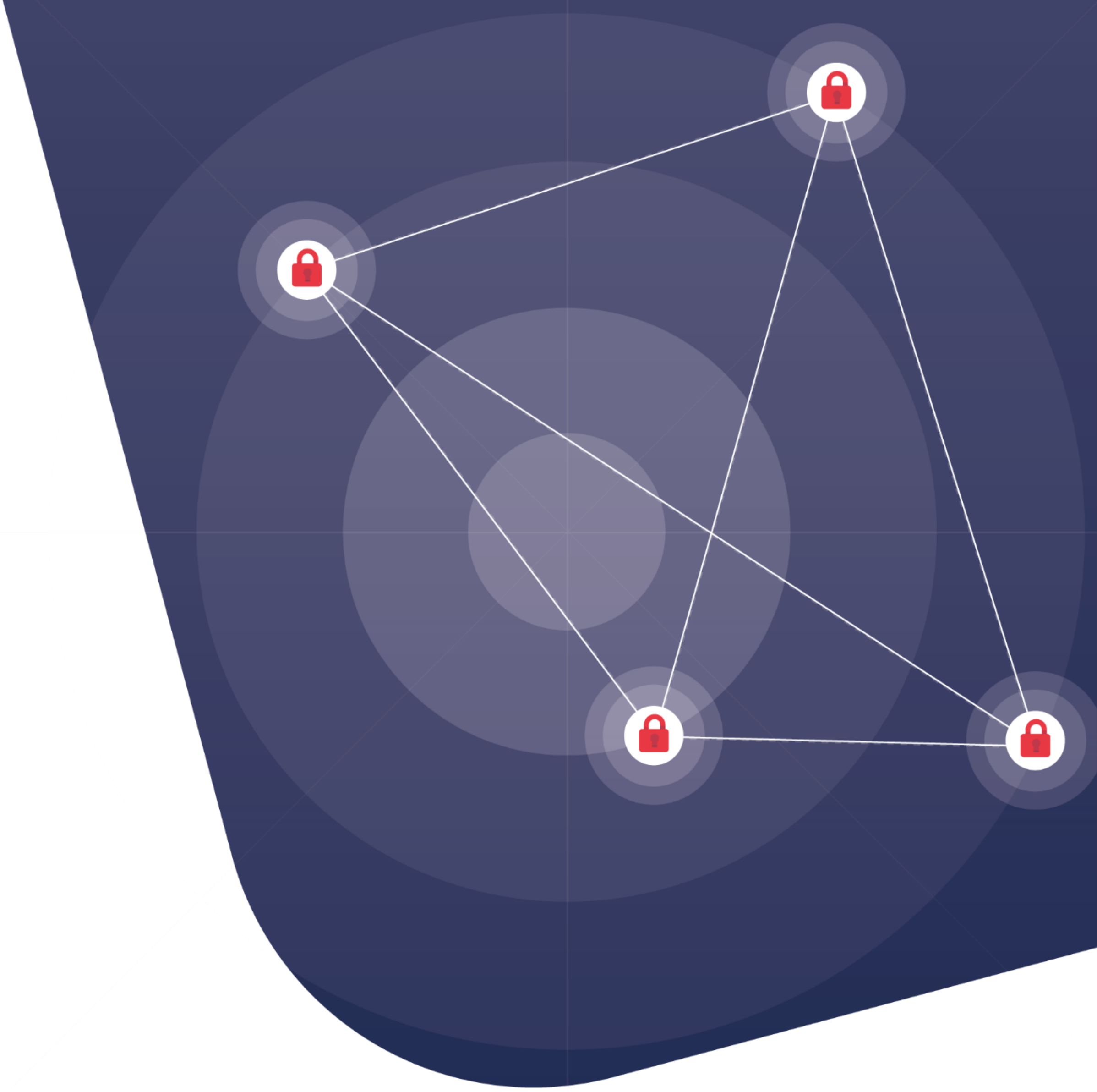

KUDELSKI IOT THINGS

APP-COSMOS SECURITY AUDIT

KUDELSKI IOT LABS

19 September 2023

DOCUMENT PROPERTIES

Version:	1.1
File Name:	Kudelski_App_Cosmos_CR-v1-1.docx
Publication Date:	19 September 2023
Confidentiality Level:	Confidential
Document Owner:	Joo Yeon Cho
Document Recipient:	Juana Orlandini
Document Status:	Proposal
Client Company Name:	Zondax

Copyright Notice

Kudelski IoT is a member of the Kudelski Group of Companies. This document is the intellectual property of Kudelski IoT and contains confidential and privileged information. The reproduction, modification, or communication to third parties (or to other than the addressee) of any part of this document is strictly prohibited without the prior written consent from Nagravision Sàrl.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1 Context and Scope

1.1.1 Initial Audit

This report describes the results of the security evaluation of:

- App-Cosmos: https://github.com/LedgerHQ/app-cosmos/pull/27 (commit be550d7).

The evaluation was performed by Kudelski IoT Security laboratory in Cheseaux-sur-Lausanne, Switzerland, between 05 September 2023 and 08 September 2023 with a total effort of 3 man-days.

The goal of the engagement was to perform a security review according to Ledger's externalized security audit framework.

The dependencies are out of scope of the review.

1.1.2 Follow-Up

After the initial report (V1.0) was delivered, Zondax addressed all vulnerabilities and weaknesses in the following codebase revision:

- Merge pull request #98 from cosmos/dev (commit 0e7a871)

Hence, the final commit of the audited repository is commit 0e7a871.

Note that the resolution of COS-#04 was clarified in Section 2.1.3.

1.2 Main Outcomes

The audit identified the following outcomes that have all been addressed in the final reviewed version (commit 0e7a871):

Security vulnerabilities: ⚠ 4 findings (including 4 LOW, see Section 2.5.1).

ID	SEVERITY	DESCRIPTION
COS-#01	LOW	Overwritten Data
COS-#02	LOW	Uninitialized Variable
COS-#03	LOW	Potential Buffer Overflow
COS-#04	LOW	Unrestricted App Permission

Weaknesses: 9 findings (see Section 2.5.2)

© 2023 Nagravision Sàrl. All Rights Reserved

WEAKNESS	DESCRIPTION
Global variable returned	Global variables should be handled carefully not to misbehave.
Missing input check	The input parameters should be validated properly.
Unmatched error code	An error code should be properly given for identifying the error condition.
Redundant code	Code should be clean and efficient.
Weird code flow	Code flow should be logical.
Incomplete test function	Test functions should be updated to match the source code.
Unmatched return type	The return type of the function should be matched.
Undeleted function declaration	A removed function should not be declared in the header file.
Lack of comments and documentation	The comments and documentation should provide information regarding the functionality, parameters and return values of the function.

Unresolved tests: **☑ 24 failed integration tests due to timeout (out of 96 tests)**

Code maturity: **☑ Fit for production**

Others:

- The application flags are not defined in the application's Makefile.

1.3 Kudelski IoT Security Laboratories

Through more than 25 years of research and security analysis of digital systems, we have developed a wide range of evaluation techniques and capabilities in order to give our clients the critical insights they need into the robustness of IoT security. Our laboratory is certified ISO/IEC 27001:2013 which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. Strict physical and logical access controls are in place to ensure the appropriate confidentiality of your information, data and samples. For more details, please visit www.kudelski-iot.com and www.nagra.com/group/at-a-glance.

1.4 Document Confidentiality Classification

This document contains sensitive information that is intended for use by a restricted group of people. Access and distribution shall be limited based upon the “need to know / need to do” principle. The recipient list can be found at the end of this report under Document Recipients.

2. AUDIT SPECIFICATION

This section follows Ledger's public audit specification that was established to perform a security audit following Ledger's standards.

2.1 Application Privileges

2.1.1 Application Flags

The applications flags used are defined in the `app/pkg/installer_s.sh`, `app/pkg/installer_x.sh`, `app/pkg/installer_stax.sh`, and `app/pkg/installer_s2.sh`, `either as`:

```
LOAD_PARAMS=(--curve secp256k1 ... --path 44/118 --path 44/60 --appFlags 0x000)
```

which enables no privileges, or as:

```
LOAD_PARAMS=(--curve secp256k1 ... --path 44/118 --path 44/60 --appFlags 0x200)
```

which enables the following privilege:

- `APPLICATION_FLAG_BOLOS_SETTINGS` (`0x200`)

Flag related to the access to the OS settings, required for the following call:

- `/deps/ledger-zxlib/app/common/app_main.c`:138

```
G_io_app.plane_mode = os_setting_get(OS_SETTING_PLANEMODE, NULL, 0);
```

According to Ledger's specification[1], the application flags should be defined in the application's Makefile.

2.1.2 Derivation Paths

In the application's Makefile, the derivation path specified is:

```
ifeq ($(COIN),ATOM)
...
APPNAME = "Cosmos"
APPPATH = "44'/118'" --path "44'/60'"
else
define error_message
```

- The coin types of Atom in BIP44[2] are indeed 118.
- The coin type of Ether in BIP44, which is 60, is set with `--path` property.

2.1.3 ChainID Parameter

According to the security guideline of Ledger[3], if the application derives keys on the hardened path `44'/60'` then the chainID parameter must be different from 0 or 1. This is addressed in the `app/src/tx_display.c as`:

[1] https://developers.ledger.com/docs/embedded-app/secure-app/#application-flags
[2] https://github.com/satoshilabs/slips/blob/ma7ster/slip-0044.md.
[3] https://developers.ledger.com/docs/embedded-app/secure-app/#restrict-apps-to-coin-specific-bip32-prefix

© 2023 Nagravision Sàrl. All Rights Reserved
Confidential

```
display_cache.is_default_chain = false;
...
    if (strcmp(outVal, COIN_DEFAULT_CHAINID) == 0) {
        // If we don't match the default chainid, switch to expert mode
        display_cache.is_default_chain = true;
...
parser_error_t tx_is_expert_mode_or_not_default_chainid(bool *expert_or_default) {
...
    bool is_default = false;
    CHECK_PARSER_ERR(is_default_chainid(&is_default))
    *expert_or_default = app_mode_expert() || !is_default;
...
}
```

This function enables the application to restrict the transaction only to the default chain.

2.2 Compilation

The compilation passed successfully without warning. The logs are in Appendix A.

© 2023 Nagravision Sàrl. All Rights Reserved

2.3 Tests

2.3.1 Unit Tests

A total of 140 unit tests from 6 test suites are written.

- 2 tests from Address
- 14 tests from JsonParserTest
- 33 tests from TxValidationTest
- 5 tests from TxParse
- 78 tests from JsonTestCases/JsonTests_Secp256
- 8 tests from JsonTestTextualCases/JsonTests_Textual

The unit tests using cpp_test compiled and passed successfully. The logs are in Appendix B.

2.3.2 Integration Tests

A total of 96 integration tests over 3 test suites are written.

The integration tests using zemu_test compiled, and the 72 tests passed successfully out of 96 tests in total. The failed test was caused by the timeout error. Since all integration tests passed in CI, we concluded that the failed test is only due to the slow test platform and not relevant to any security issue.

2.4 Static Analysis

2.4.1 Scan-build

Scan-build did not identify any critical findings.

```
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
scan-build: Removing directory '/home/joo/projects/zondax/app-cosmos-main/audit_logs/scan-
build-result.txt/2023-09-04-193858-16780-1' because it contains no reports.
scan-build: No bugs found.
```

2.4.2 Semgrep

Semgrep (v1.20.0) did not identify any findings.

```
{"errors": [], "paths": {"scanned": ["app/src/.gitignore", "app/src/addr.c",
"app/src/addr.h", "app/src/apdu_handler.c", "app/src/cbor/cbor_parser_helper.c",
"app/src/cbor/cbor_parser_helper.h", "app/src/chain_config.c", "app/src/chain_config.h",
"app/src/coin.h", "app/src/common/actions.c", "app/src/common/actions.h",
"app/src/common/main.c", "app/src/common/parser.h", "app/src/common/parser_common.h",
"app/src/common/tx.c", "app/src/common/tx.h", "app/src/crypto.c", "app/src/crypto.h",
"app/src/json/json_parser.c", "app/src/json/json_parser.h", "app/src/parser.c",
"app/src/parser_impl.c", "app/src/parser_impl.h", "app/src/parser_txdef.h",
"app/src/secret.c", "app/src/secret.h", "app/src/tx_display.c", "app/src/tx_display.h",
"app/src/tx_parser.c", "app/src/tx_parser.h", "app/src/tx_validate.c",
"app/src/tx_validate.h"], "skipped": []}, "results": [], "version": "1.20.0"}
```

2.4.3 Cppcheck

Cppcheck (v1.90) did not identify any critical findings.

```
Checking app/src/addr.c ...
1/15 files checked 2% done
Checking app/src/apdu_handler.c ...
Checking app/src/apdu_handler.c: DEBUG...
Checking app/src/apdu_handler.c: LEDGER_SPECIFIC...
Checking app/src/apdu_handler.c: TARGET_NANOS...
Checking app/src/apdu_handler.c: TARGET_STAX...
2/15 files checked 10% done
Checking app/src/cbor/cbor_parser_helper.c ...
3/15 files checked 15% done
Checking app/src/chain_config.c ...
4/15 files checked 17% done
Checking app/src/common/actions.c ...
5/15 files checked 18% done
Checking app/src/common/main.c ...
6/15 files checked 19% done
Checking app/src/common/tx.c ...
Checking app/src/common/tx.c: TARGET_NANOS...
Checking app/src/common/tx.c: TARGET_NANOS2;TARGET_NANOX;TARGET_STAX...
Checking app/src/common/tx.c: TARGET_NANOS;TARGET_NANOS2;TARGET_NANOX;TARGET_STAX...
7/15 files checked 23% done
Checking app/src/crypto.c ...
8/15 files checked 30% done
Checking app/src/json/json_parser.c ...
Checking app/src/json/json_parser.c: APP_TESTING...
Checking app/src/json/json_parser.c: LEDGER_SPECIFIC...
Checking app/src/json/json_parser.c: TARGET_NANOS...
Checking app/src/json/json_parser.c: TARGET_STAX...
9/15 files checked 38% done
Checking app/src/parser.c ...
Checking app/src/parser.c: LEDGER_SPECIFIC...
Checking app/src/parser.c: TARGET_NANOS...
Checking app/src/parser.c: TARGET_STAX...
10/15 files checked 56% done
Checking app/src/parser_impl.c ...
Checking app/src/parser_impl.c: LEDGER_SPECIFIC...
Checking app/src/parser_impl.c: TARGET_NANOS...
Checking app/src/parser_impl.c: TARGET_STAX...
11/15 files checked 62% done
Checking app/src/secret.c ...
Checking app/src/secret.c: APP_SECRET_MODE_ENABLED...
12/15 files checked 64% done
Checking app/src/tx_display.c ...
Checking app/src/tx_display.c: APP_TESTING...
Checking app/src/tx_display.c: LEDGER_SPECIFIC...
Checking app/src/tx_display.c: TARGET_NANOS...
Checking app/src/tx_display.c: TARGET_STAX...
13/15 files checked 85% done
Checking app/src/tx_parser.c ...
Checking app/src/tx_parser.c: LEDGER_SPECIFIC...
Checking app/src/tx_parser.c: TARGET_NANOS...
Checking app/src/tx_parser.c: TARGET_STAX...
14/15 files checked 95% done
Checking app/src/tx_validate.c ...
Checking app/src/tx_validate.c: LEDGER_SPECIFIC...
Checking app/src/tx_validate.c: TARGET_NANOS...
Checking app/src/tx_validate.c: TARGET_STAX...
15/15 files checked 100% done
```

2.4.4 CodeQL

CodeQL (v2.13.0) ran using the `codeql/cpp-queries:codeql-suites/cpp-security-and-quality.qls` query suite did not identify any outstanding finding under scope.

The CodeQL output is in Appendix C.

© 2023 Nagravision Sàrl. All Rights Reserved

2.5 Manual Code Review

2.5.1 Vulnerabilities

This section lists the security vulnerabilities identified during the audit.

COS-#01 Overwritten Data

Severity. LOW

Impact. Functionality

File locations. app/src/crypto.c: 73

```
__Z_INLINE zxerr_t compressPubkey(const uint8_t *pubkey, uint16_t pubkeyLen, uint8_t *output, uint16_t outputLen) {

...

    // Format pubkey

    for (int i = 0; i < 32; i++) {

        output[i] = pubkey[64 - i];

    }

    if ((pubkey[32] & 1) != 0) {

        output[31] |= 0x80;

    }


    MEMCPY(output, pubkey, PK_LEN_SECP256K1);

    output[0] = pubkey[64] & 1 ? 0x03 : 0x02; // "Compress" public key in place

    return zxerr_ok;

}
```

Description.

In the function `compressPubkey`, the array `pubkey[64..33]` is stored on the array `output[0..31]` and then `pubkey[0..32]` is copied to `output[0..32]` by `MEMCPY`, which overwrites the previous stored data in `output[0..31]`.

Recommendation. Ensure the public key compressing process is correct. Add a comment to explain why.

COS-#02 Uninitialized Variable

Severity. **LOW**

Impact. Functionality

File locations. app/src/crypto.c: 32

```
address_encoding_e encoding;
...
static zxerr_t crypto_hashBuffer(const uint8_t *input, const uint16_t
inputLen, uint8_t *output, uint16_t outputLen) {

    switch (encoding) {
        case BECH32_COSMOS: {
        ...
        case BECH32_ETH: {
        ...
        default:
            return zxerr_unknown;
    }
    return zxerr_ok;
}
```

Description. The global variable `encoding` is declared but not initialized. Later, it is used in the `switch` statement without assignment.

Recommendation. Initialize encoding by the default value. Assuming that a global variable is initialized with zero by default, which is ok since `BECH32_COSMOS = 0` but it is recommended to remove any ambiguity in the code if possible.

COS-#03 Potential Buffer Overflow

Severity. LOW

Impact. Functionality

File locations. app/src/apdu_handle.c: 84

```
__Z_INLINE void extractHDPath(uint32_t rx, uint32_t offset) {
    if ((rx - offset) < sizeof(uint32_t) * HDPATH_LEN_DEFAULT) {
        THROW(APDU_CODE_WRONG_LENGTH);
    }
...
```

Description. The input parameters `rx` and `offset` are of type `uint32_t`. If `offset` is greater than `rx`, then, `rx - offset` can be casted as a non-negative big number which unintentionally satisfies the condition.

In comparison, in line 65, the following code is used to ensure that `rx` is greater than `offset`.

```
    if (rx < offset + 1) {
        THROW(APDU_CODE_DATA_INVALID);
    }
```

Recommendation. Ensure the buffer overflow error never occurs.

COS-#04 Unrestricted App Permission

Severity. **LOW**

Impact. Functionality

File locations. app/src/parser.c

```
parser_error_t parser_validate(const parser_context_t *ctx) {
    if (ctx->tx_obj->tx_type == tx_json) {
          CHECK_PARSER_ERR(tx_validate(&parser_tx_obj.tx_json.json))
    }
    // Iterate through all items to check that all can be shown and are
valid
    uint8_t numItems = 0;
    CHECK_PARSER_ERR(parser_getNumItems(ctx, &numItems))
...
    return parser_ok;
}
```

Description. The security guideline of Ledger[4] says that if your application derives keys on the hardened path 44'/60' then the chainID parameter must be different from 0 or 1. However, such restriction is not observed in the source code.

Recommendation. Validate the chain id to avoid replaying transactions broadcoast on Ethereum-like chains on Ethereum.

[4] https://developers.ledger.com/docs/embedded-app/secure-app/#restrict-apps-to-coin-specific-bip32-prefix

2.5.2 Weaknesses

This section lists the security weaknesses identified in the audit. A weakness is not exploitable in the current state of the codebase but can lead to the introduction of vulnerabilities during maintenance.

Global variable returned

Global variables are not supposed to be used as input parameters nor a return value. However, the function `extractHRP` returns `bech32_hrp_len` which is defined in `crypto.c` Furthermore, in the function `extractHDPath_HRP`, the return value of `extractHRP` is not used, instead, `bech32_hrp_len` itself is used.

- `app/src/crypto.c`

```
30   uint8_t bech32_hrp_len;
     char bech32_hrp[MAX_BECH32_HRP_LEN + 1];
```

- `app/src/apdu_handler.c`

```
65   __Z_INLINE uint8_t extractHRP(uint32_t rx, uint32_t offset) {
     ...
         return bech32_hrp_len;
     }
     ...
106  static void extractHDPath_HRP(uint32_t rx, uint32_t offset) {
     ...
         extractHRP(rx, offset + sizeof(uint32_t) * HDPATH_LEN_DEFAULT);
         encoding = checkChainConfig(hdPath[1], bech32_hrp,
     bech32_hrp_len);
```

Missing input check

The input parameters are not validated in the following functions, while the other functions do check.

- `app/src/cbor/cbor_parser_helper.c`

```
37   static parser_error_t cbor_check_optFields(CborValue *data,
     Cbor_container *container) {
     ...
69   static parser_error_t cbor_check_screen(CborValue *data,
     Cbor_container *container) {
```

Unless otherwise, it is recommended to add the following code to the functions above.

```
if (data == NULL || container == NULL) {
    return parser_unexpected_value;
}
```

© 2023 Nagravision Sàrl. All Rights Reserved

Unmatched error code

The error code is not matched or inconsistent with the code flow.

- app/src/crypto.c

```
if (pubkey == NULL || output == NULL ||
        pubkeyLen != PK_LEN_SECP256K1_UNCOMPRESSED || outputLen <
PK_LEN_SECP256K1) {
            return zxerr_unknown;
```

For consistency, the error code `zxerr_invalid_crypto_settings` may be used instead.

Redundant code

The variable `displayIdx` is of type `uint8_t`. Hence, no need to check it is negative or not.

- app/src/parser.c

```
    if (displayIdx < 0 || displayIdx >= numItems) {
        return parser_display_idx_out_of_range;
    };
```

- app/src/tx_display.c

```
    if (displayIdx < 0 || displayIdx >= numItems) {
        return parser_display_idx_out_of_range;
    };
```

Weird code flow

The variable `parser_tx_obj.tx_json.json.tokens[amountToken + 2].start` is validated after it is used. Also, `parser_tx_obj.tx_json.json.tokens[amountToken + 4].start` is not validated.

- app/src/parser.c

```
const char *amountPtr = parser_tx_obj.tx_json.tx +
parser_tx_obj.tx_json.json.tokens[amountToken + 2].start;
if (parser_tx_obj.tx_json.json.tokens[amountToken + 2].start < 0) {
        return parser_unexpected_buffer_end;
    }
```

Incomplete test function

The function `parser_parse` is declared with 4 input parameters. However, in `parser_parse.cpp`, this function is called with 3 input parameters, which leads to the compile failure of the unit test and the fuzzing test.

The fuzzing target code is located in `fuzzing`, not `fuzz`.

© 2023 Nagravision Sàrl. All Rights Reserved

- fuzzing/parser_parse.cpp

```
    rc = parser_parse(&ctx, data, size);
```

- app/src/fuzzing/parser_parse.cpp

```
parser_error_t parser_parse(parser_context_t *ctx,
                            const uint8_t *data,
                            size_t dataLen,
                            parser_tx_t *tx_obj);
```

- deps/ledger-zxlib/dockerized_build.mk

```
.PHONY: fuzz
fuzz: fuzz_build
      ./fuzz/run-fuzzers.py
.PHONY: fuzz_crash
fuzz_crash: FUZZ_LOGGING=1
fuzz_crash: fuzz_build
      ./fuzz/run-fuzz-crashes.py
```

- CMakeLists.txt

```
add_executable(fuzz-${target}
${CMAKE_CURRENT_SOURCE_DIR}/fuzz/${target}.cpp)
```

It is recommended to make the parameters and folder name matched to proceed the unit and fuzzing tests.

Unmatched return type

The function `is_default_chainid` returns `bool`, but if there is an error, then `CHECK_PARSER_ERR` returns `parser_error_t`.

The function `get_subitem_count` returns `uint8_t`, but if there is an error, then `CHECK_PARSER_ERR` returns `parser_error_t`.

The name of the function `tx_is_expert_mode` is confusing. It should be `tx_is_expert_mode_or_not_default_chainid` or something like that.

- app/src/tx_display.c

```
__Z_INLINE bool is_default_chainid() {
    CHECK_PARSER_ERR(tx_indexRootFields())
    return display_cache.is_default_chain;
}
bool tx_is_expert_mode() {
    return app_mode_expert() || !is_default_chainid();
}
__Z_INLINE uint8_t get_subitem_count(root_item_e root_item) {
    CHECK_PARSER_ERR(tx_indexRootFields())
```

Undeleted function declaration

The function `crypto_set_hrp` is removed from `crypto.c` in PR#27, but its declaration in `crypto.h` is not removed yet.

- `app/src/crypto.h`

```
void crypto_set_hrp(char *p);
```

Lack of comments and documentation

The lack of comments and documentation makes it harder to understand the code, and can result in the developer misusing a function, thus causing bugs and/or security issues. Function documentation should explain the goal, input arguments, output arguments and returned value.

© 2023 Nagravision Sàrl. All Rights Reserved

2.6 Fuzzing

2.6.1 Methodology

Zondax used libfuzzer to build one fuzz target.

The target, named `parser_parse.cpp`, tests the applications parser's `parser_parse`, `parser_validate`, `parser_getNumItems` and `parser_getItem` functions with random values.

2.6.2 Source code

The source code of the fuzzer is provided in the `fuzz` directory of the Cosmos repository. The fuzzer was built and run using `make fuzz_build` and `make fuzz`, respectively.

2.6.3 Coverage

The parser code is in fuzz/parser_parse.cpp. This file has the following coverage:

Filename	Function Coverage	Line Coverage	Region Coverage
zxerror.h	0.00% (0/1)	0.00% (0/33)	0.00% (0/1)
zxformat.h	5.00% (1/20)	3.74% (15/401)	29.63% (8/27)
zxmacros.h	0.00% (0/2)	0.00% (0/9)	0.00% (0/2)
cbor.h	0.00% (0/56)	0.00% (0/182)	0.00% (0/56)
parser_parse.cpp	100.00% (1/1)	36.84% (21/57)	37.50% (6/16)
Totals	**2.50% (2/80)**	**5.28% (36/682)**	**13.73% (14/102)**

The region and line which are not covered are not critical. We believe that the coverage rate is good enough and covers the parser well.

The full coverage report can be generated by following the instructions in the README we provided.

2.6.4 Findings

Running the fuzzer on the parser shows a growing coverage. While fuzzing these targets, we did not identify any critical findings.

2.6.5 ClusterFuzzLite

ClusterFuzzLite allows the integration of the fuzzing process into the CI of the project. For GitHub, it is made with the help of GitHub actions. A pull request should be made to integrate such GitHub action in the Cosmos repository.

3. CONCLUSION

The Cosmos codebase presented a few vulnerabilities and weaknesses that are identified in Section 2.5.1, and those vulnerabilities and weaknesses were all addressed by Zondax in the follow-up revision of the codebase.

Based on our results, the revision codebase meets adequate code maturity for production.

.

DOCUMENT RECIPIENTS

NAME	POSITION	CONTACT INFORMATION
Fernando Theirs	Technical Contact	fernando@zondax.ch
Juana Orlandini	Project Manager	juana.orlandini@zondax.ch

KUDELSKI IOT CONTACTS

NAME	POSITION	ADDRESS, PHONE, EMAIL
Joo Yeon Cho	Blockchain Expert	Dingolfinger Strasse 15 81673, Munich Germany Joo.cho@kudelskisecurity.com
Adel Qasem	Security Engineer	Ch. de la Chapelle 4-6 1033 Cheseaux Switzerland adel.qasem@nagra.com
Gerrit Holtrup	Principal Security Engineer	Ch. de la Chapelle 4-6 1033 Cheseaux Switzerland +41217320653 Gerrit.Holtrup@nagra.com
Pascal Aubry	Senior Security Evaluations Lab Manager	Ch. de la Chapelle 4-6 1033 Cheseaux Switzerland +41217320653 pascal.aubry@nagra.com

ACRONYMS

ACRONYM	DEFINITION

A. COMPILATION LOGS

```
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
make[1]: Entering directory '/home/joo/projects/zondax/app-cosmos-main'
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
Removing output files
docker run "-t" "-i" --rm -e
SCP_PRIVKEY=ff701d781f43ce106f72dc26a46b6a83e053b5d07bb3d4ceab79c91ca822a6
6b -e SDK_VARNAME=NANOSP_SDK -e TARGET=nanos2 -u 1000:1000 -v
/home/joo/projects/zondax/app-cosmos-main:/app -e SUPPORT_SR25519= -e
SUBSTRATE_PARSER_FULL= -e DISABLE_PREVIOUS= -e DISABLE_CURRENT= -e COIN= -
e APP_TESTING= zondax/ledger-app-builder:ledger-
9b3d174a6a4eed7e5196b431a3b68ca9013433a9 "make clean"

--------------------------------------
Zondax BOLOS container - zondax.ch
--------------------------------------

BOLOS_SDK=/opt/nanosplus-secure-sdk

"Calling app Makefile for target clean"
COIN= make -C app clean
make[1]: Entering directory '/app/app'
************ TARGET_NAME  = [TARGET_NANOS2]
COIN  = [ATOM]
TARGET_NAME  = [TARGET_NANOS2]
ICONNAME  = [/app/app/nanox_icon.gif]
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
No rust code
rm -fr build bin debug
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
make[1]: Entering directory '/home/joo/projects/zondax/app-cosmos-main'
```

© 2023 Nagravision Sàrl. All Rights Reserved

```
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
docker run "-t" "-i" --rm -e
SCP_PRIVKEY=ff701d781f43ce106f72dc26a46b6a83e053b5d07bb3d4ceab79c91ca822a6
6b -e SDK_VARNAME=NANOS_SDK -e TARGET=nanos -u 1000:1000 -v
/home/joo/projects/zondax/app-cosmos-main:/app -e SUPPORT_SR25519= -e
SUBSTRATE_PARSER_FULL= -e DISABLE_PREVIOUS= -e DISABLE_CURRENT= -e COIN= -
e APP_TESTING= zondax/ledger-app-builder:ledger-
9b3d174a6a4eed7e5196b431a3b68ca9013433a9 "make -j 8"

--------------------------------------
Zondax BOLOS container - zondax.ch
--------------------------------------

BOLOS_SDK=/opt/nanos-secure-sdk

make -C app
make[1]: Entering directory '/app/app'
TARGET_NAME=TARGET_NANOS TARGET_ID=0x31100004 TARGET_VERSION=2.1.0
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
************ TARGET_NAME  = [TARGET_NANOS]
COIN  = [ATOM]
TARGET_NAME  = [TARGET_NANOS]
ICONNAME  = [/app/app/nanos_icon.gif]
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
Prepare directories
[GLYPH] Compiling...
[CC]   build/nanos/obj/actions.o
[CC]   build/nanos/obj/addr.o
[CC]   build/nanos/obj/apdu_handler.o
[CC]   build/nanos/obj/app_main.o
[CC]   build/nanos/obj/app_mode.o
[CC]   build/nanos/obj/bagl.o
[CC]   build/nanos/obj/bagl_fonts.o
[CC]   build/nanos/obj/bagl_glyphs.o
[CC]   build/nanos/obj/base58.o
[CC]   build/nanos/obj/base64.o
[CC]   build/nanos/obj/bech32.o
[CC]   build/nanos/obj/bignum.o
```

```
[CC]   build/nanos/obj/buffering.o
[CC]   build/nanos/obj/cbor_parser_helper.o
[CC]   build/nanos/obj/cborparser.o
[CC]   build/nanos/obj/cborvalidation.o
[CC]   build/nanos/obj/chain_config.o
[CC]   build/nanos/obj/checks.o
[CC]   build/nanos/obj/crypto.o
[AS]   build/nanos/obj/cx_stubs.o
[CC]   build/nanos/obj/glyphs.o
[CC]   build/nanos/obj/hexutils.o
[CC]   build/nanos/obj/jsmn.o
[CC]   build/nanos/obj/json_parser.o
[CC]   build/nanos/obj/ledger_protocol.o
[CC]   build/nanos/obj/main.o
[CC]   build/nanos/obj/os.o
[CC]   build/nanos/obj/os_io_seproxyhal.o
[CC]   build/nanos/obj/os_io_task.o
[CC]   build/nanos/obj/os_io_usb.o
[CC]   build/nanos/obj/os_printf.o
[CC]   build/nanos/obj/parser.o
[CC]   build/nanos/obj/parser_impl.o
[CC]   build/nanos/obj/pic.o
[CC]   build/nanos/obj/secret.o
[CC]   build/nanos/obj/segwit_addr.o
[CC]   build/nanos/obj/sigutils.o
[AS]   build/nanos/obj/svc_call.o
[AS]   build/nanos/obj/svc_cx_call.o
[CC]   build/nanos/obj/syscalls.o
[CC]   build/nanos/obj/timeutils.o
[CC]   build/nanos/obj/tx.o
[CC]   build/nanos/obj/tx_display.o
[CC]   build/nanos/obj/tx_parser.o
[CC]   build/nanos/obj/tx_validate.o
[CC]   build/nanos/obj/u2f_impl.o
[CC]   build/nanos/obj/u2f_io.o
[CC]   build/nanos/obj/usbd_ccid_cmd.o
[CC]   build/nanos/obj/usbd_ccid_core.o
[CC]   build/nanos/obj/usbd_ccid_if.o
[CC]   build/nanos/obj/usbd_conf.o
[CC]   build/nanos/obj/usbd_core.o
[CC]   build/nanos/obj/usbd_ctlreq.o
[CC]   build/nanos/obj/usbd_hid.o
[CC]   build/nanos/obj/usbd_impl.o
[CC]   build/nanos/obj/usbd_ioreq.o
[CC]   build/nanos/obj/ux_flow_engine.o
[CC]   build/nanos/obj/ux_layout_bb.o
[CC]   build/nanos/obj/ux_layout_bn.o
[CC]   build/nanos/obj/ux_layout_bnn.o
[CC]   build/nanos/obj/ux_layout_bnnn.o
```

```
[CC]   build/nanos/obj/ux_layout_nn.o
[CC]   build/nanos/obj/ux_layout_nnbnn.o
[CC]   build/nanos/obj/ux_layout_nnn.o
[CC]   build/nanos/obj/ux_layout_nnnn.o
[CC]   build/nanos/obj/ux_layout_paging.o
[CC]   build/nanos/obj/ux_layout_paging_compute.o
[CC]   build/nanos/obj/ux_layout_pb.o
[CC]   build/nanos/obj/ux_layout_pbb.o
[CC]   build/nanos/obj/ux_layout_pbn.o
[CC]   build/nanos/obj/ux_layout_pn.o
[CC]   build/nanos/obj/ux_layout_pnn.o
[CC]   build/nanos/obj/ux_layout_utils.o
[CC]   build/nanos/obj/ux_legacy.o
[CC]   build/nanos/obj/ux_menulist.o
[CC]   build/nanos/obj/ux_stack.o
[CC]   build/nanos/obj/view.o
[CC]   build/nanos/obj/view_nano.o
[CC]   build/nanos/obj/view_s.o
[CC]   build/nanos/obj/view_stax.o
[CC]   build/nanos/obj/view_x.o
[CC]   build/nanos/obj/zxformat.o
[CC]   build/nanos/obj/zxmacros.o
[CC]   build/nanos/obj/zxutils_ledger.o
[LINK] build/nanos/bin/app.elf
[CP] build/nanos/bin/app.elf => bin/app.elf
[CP] build/nanos/bin/app.hex => bin/app.hex
[CP] build/nanos/dbg/app.map => debug/app.map
[CP] build/nanos/dbg/app.asm => debug/app.asm
[CP] build/nanos/bin/app.apdu => bin/app.apdu
[CP] build/nanos/bin/app.sha256 => bin/app.sha256
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
make[1]: Entering directory '/home/joo/projects/zondax/app-cosmos-main'
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
docker run "-t" "-i" --rm -e
SCP_PRIVKEY=ff701d781f43ce106f72dc26a46b6a83e053b5d07bb3d4ceab79c91ca822a6
6b -e SDK_VARNAME=NANOX_SDK -e TARGET=nanox -u 1000:1000 -v
/home/joo/projects/zondax/app-cosmos-main:/app -e SUPPORT_SR25519= -e
SUBSTRATE_PARSER_FULL= -e DISABLE_PREVIOUS= -e DISABLE_CURRENT= -e COIN= -
e APP_TESTING= zondax/ledger-app-builder:ledger-
9b3d174a6a4eed7e5196b431a3b68ca9013433a9 "make -j 8"
```

```
--------------------------------------
Zondax BOLOS container - zondax.ch
--------------------------------------

BOLOS_SDK=/opt/nanox-secure-sdk

make -C app
make[1]: Entering directory '/app/app'
************ TARGET_NAME  = [TARGET_NANOX]
COIN  = [ATOM]
TARGET_NAME  = [TARGET_NANOX]
ICONNAME  = [/app/app/nanox_icon.gif]
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
Prepare directories
[GLYPH] Compiling...
[CC]   build/nanox/obj/actions.o
[CC]   build/nanox/obj/addr.o
[CC]   build/nanox/obj/apdu_handler.o
[CC]   build/nanox/obj/app_main.o
[CC]   build/nanox/obj/app_mode.o
[CC]   build/nanox/obj/bagl.o
[CC]   build/nanox/obj/bagl_animate.o
[CC]   build/nanox/obj/bagl_fonts.o
[CC]   build/nanox/obj/bagl_glyphs.o
[CC]   build/nanox/obj/base58.o
[CC]   build/nanox/obj/base64.o
[CC]   build/nanox/obj/bech32.o
[CC]   build/nanox/obj/bignum.o
[CC]   build/nanox/obj/ble_gap_aci.o
[CC]   build/nanox/obj/ble_gatt_aci.o
[CC]   build/nanox/obj/ble_hal_aci.o
[CC]   build/nanox/obj/ble_hci_le.o
[CC]   build/nanox/obj/ble_l2cap_aci.o
[CC]   build/nanox/obj/buffering.o
[CC]   build/nanox/obj/cbor_parser_helper.o
[CC]   build/nanox/obj/cborparser.o
[CC]   build/nanox/obj/cborvalidation.o
[CC]   build/nanox/obj/chain_config.o
[CC]   build/nanox/obj/checks.o
[CC]   build/nanox/obj/crypto.o
[AS]   build/nanox/obj/cx_stubs.o
[CC]   build/nanox/obj/glyphs.o
[CC]   build/nanox/obj/hexutils.o
[CC]   build/nanox/obj/jsmn.o
[CC]   build/nanox/obj/json_parser.o
[CC]   build/nanox/obj/ledger_ble.o
[CC]   build/nanox/obj/ledger_protocol.o
```

© 2023 Nagravision Sàrl. All Rights Reserved
Confidential

```
[CC]    build/nanox/obj/main.o
[CC]    build/nanox/obj/os.o
[CC]    build/nanox/obj/os_io_seproxyhal.o
[CC]    build/nanox/obj/os_io_task.o
[CC]    build/nanox/obj/os_io_usb.o
[CC]    build/nanox/obj/os_printf.o
[CC]    build/nanox/obj/osal.o
[CC]    build/nanox/obj/parser.o
[CC]    build/nanox/obj/parser_impl.o
[CC]    build/nanox/obj/pic.o
[CC]    build/nanox/obj/secret.o
[CC]    build/nanox/obj/segwit_addr.o
[CC]    build/nanox/obj/sigutils.o
[CC]    build/nanox/obj/stack_protector.o
[AS]    build/nanox/obj/stack_protector_init.o
[AS]    build/nanox/obj/svc_call.o
[AS]    build/nanox/obj/svc_cx_call.o
[CC]    build/nanox/obj/syscalls.o
[CC]    build/nanox/obj/timeutils.o
[CC]    build/nanox/obj/tx.o
[CC]    build/nanox/obj/tx_display.o
[CC]    build/nanox/obj/tx_parser.o
[CC]    build/nanox/obj/tx_validate.o
[CC]    build/nanox/obj/u2f_impl.o
[CC]    build/nanox/obj/u2f_io.o
[CC]    build/nanox/obj/usbd_ccid_cmd.o
[CC]    build/nanox/obj/usbd_ccid_core.o
[CC]    build/nanox/obj/usbd_ccid_if.o
[CC]    build/nanox/obj/usbd_conf.o
[CC]    build/nanox/obj/usbd_core.o
[CC]    build/nanox/obj/usbd_ctlreq.o
[CC]    build/nanox/obj/usbd_hid.o
[CC]    build/nanox/obj/usbd_impl.o
[CC]    build/nanox/obj/usbd_ioreq.o
[CC]    build/nanox/obj/ux_flow_engine.o
[CC]    build/nanox/obj/ux_layout_bb.o
[CC]    build/nanox/obj/ux_layout_bn.o
[CC]    build/nanox/obj/ux_layout_bnn.o
[CC]    build/nanox/obj/ux_layout_bnnn.o
[CC]    build/nanox/obj/ux_layout_nn.o
[CC]    build/nanox/obj/ux_layout_nnbnn.o
[CC]    build/nanox/obj/ux_layout_nnn.o
[CC]    build/nanox/obj/ux_layout_nnnn.o
[CC]    build/nanox/obj/ux_layout_pages.o
[CC]    build/nanox/obj/ux_layout_paging.o
[CC]    build/nanox/obj/ux_layout_paging_compute.o
[CC]    build/nanox/obj/ux_layout_pb.o
[CC]    build/nanox/obj/ux_layout_pbb.o
[CC]    build/nanox/obj/ux_layout_pbn.o
```

```
[CC]   build/nanox/obj/ux_layout_pn.o
[CC]   build/nanox/obj/ux_layout_pnn.o
[CC]   build/nanox/obj/ux_layout_utils.o
[CC]   build/nanox/obj/ux_legacy.o
[CC]   build/nanox/obj/ux_menulist.o
[CC]   build/nanox/obj/ux_stack.o
[CC]   build/nanox/obj/view.o
[CC]   build/nanox/obj/view_nano.o
[CC]   build/nanox/obj/view_s.o
[CC]   build/nanox/obj/view_stax.o
[CC]   build/nanox/obj/view_x.o
[CC]   build/nanox/obj/zxformat.o
[CC]   build/nanox/obj/zxmacros.o
[CC]   build/nanox/obj/zxutils_ledger.o
[LINK] build/nanox/bin/app.elf
[CP] build/nanox/bin/app.elf => bin/app.elf
[CP] build/nanox/bin/app.hex => bin/app.hex
[CP] build/nanox/dbg/app.map => debug/app.map
[CP] build/nanox/dbg/app.asm => debug/app.asm
[CP] build/nanox/bin/app.apdu => bin/app.apdu
[CP] build/nanox/bin/app.sha256 => bin/app.sha256
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
make[1]: Entering directory '/home/joo/projects/zondax/app-cosmos-main'
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
docker run "-t" "-i" --rm -e
SCP_PRIVKEY=ff701d781f43ce106f72dc26a46b6a83e053b5d07bb3d4ceab79c91ca822a6
6b -e SDK_VARNAME=NANOSP_SDK -e TARGET=nanos2 -u 1000:1000 -v
/home/joo/projects/zondax/app-cosmos-main:/app -e SUPPORT_SR25519= -e
SUBSTRATE_PARSER_FULL= -e DISABLE_PREVIOUS= -e DISABLE_CURRENT= -e COIN= -
e APP_TESTING= zondax/ledger-app-builder:ledger-
9b3d174a6a4eed7e5196b431a3b68ca9013433a9 "make -j 8"

--------------------------------------
Zondax BOLOS container - zondax.ch
--------------------------------------

BOLOS_SDK=/opt/nanosplus-secure-sdk

make -C app
make[1]: Entering directory '/app/app'
************ TARGET_NAME  = [TARGET_NANOS2]
```

```
COIN  = [ATOM]
TARGET_NAME  = [TARGET_NANOS2]
ICONNAME  = [/app/app/nanox_icon.gif]
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
Prepare directories
...
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
make[1]: Entering directory '/home/joo/projects/zondax/app-cosmos-main'
USERID                : 1000
GROUPID               : 1000
TESTS_ZEMU_DIR        : /home/joo/projects/zondax/app-cosmos-
main/tests_zemu
EXAMPLE_VUE_DIR       : /home/joo/projects/zondax/app-cosmos-
main/example_vue
TESTS_JS_DIR          :
TESTS_JS_PACKAGE      :
docker run "-t" "-i" --rm -e
SCP_PRIVKEY=ff701d781f43ce106f72dc26a46b6a83e053b5d07bb3d4ceab79c91ca822a6
6b -e SDK_VARNAME=STAX_SDK -e TARGET=stax -u 1000:1000 -v
/home/joo/projects/zondax/app-cosmos-main:/app -e SUPPORT_SR25519= -e
SUBSTRATE_PARSER_FULL= -e DISABLE_PREVIOUS= -e DISABLE_CURRENT= -e COIN= -
e APP_TESTING= zondax/ledger-app-builder:ledger-
9b3d174a6a4eed7e5196b431a3b68ca9013433a9 "make -j 8"

--------------------------------------
Zondax BOLOS container - zondax.ch
--------------------------------------

BOLOS_SDK=/opt/stax-secure-sdk

make -C app
make[1]: Entering directory '/app/app'
************ TARGET_NAME  = [TARGET_STAX]
COIN  = [ATOM]
TARGET_NAME  = [TARGET_STAX]
ICONNAME  = [/app/app/stax_icon.gif]
BOLOS_ENV is not set: falling back to CLANGPATH and GCCPATH
CLANGPATH is not set: clang will be used from PATH
GCCPATH is not set: arm-none-eabi-* will be used from PATH
Prepare directories
[GLYPH] Compiling...
[CC]   build/stax/obj/actions.o
[CC]   build/stax/obj/addr.o
[CC]   build/stax/obj/apdu_handler.o
[CC]   build/stax/obj/app_main.o
[CC]   build/stax/obj/app_mode.o
```

© 2023 Nagravision Sàrl. All Rights Reserved

```
[CC]   build/stax/obj/base58.o
[CC]   build/stax/obj/base64.o
[CC]   build/stax/obj/bech32.o
[CC]   build/stax/obj/bignum.o
[CC]   build/stax/obj/ble_gap_aci.o
[CC]   build/stax/obj/ble_gatt_aci.o
[CC]   build/stax/obj/ble_hal_aci.o
[CC]   build/stax/obj/ble_hci_le.o
[CC]   build/stax/obj/ble_l2cap_aci.o
[CC]   build/stax/obj/buffering.o
[CC]   build/stax/obj/cbor_parser_helper.o
[CC]   build/stax/obj/cborparser.o
[CC]   build/stax/obj/cborvalidation.o
[CC]   build/stax/obj/chain_config.o
[CC]   build/stax/obj/checks.o
[CC]   build/stax/obj/crypto.o
[AS]   build/stax/obj/cx_stubs.o
[CC]   build/stax/obj/generate_data_test.o
[CC]   build/stax/obj/glyphs.o
[CC]   build/stax/obj/hexutils.o
[CC]   build/stax/obj/jsmn.o
[CC]   build/stax/obj/json_parser.o
[CC]   build/stax/obj/ledger_ble.o
[CC]   build/stax/obj/ledger_protocol.o
[CC]   build/stax/obj/main.o
[CC]   build/stax/obj/nbgl_bottom_button.o
[CC]   build/stax/obj/nbgl_draw.o
[CC]   build/stax/obj/nbgl_fonts.o
[CC]   build/stax/obj/nbgl_layout.o
[CC]   build/stax/obj/nbgl_navigation.o
[CC]   build/stax/obj/nbgl_obj.o
[CC]   build/stax/obj/nbgl_obj_keyboard.o
[CC]   build/stax/obj/nbgl_obj_keypad.o
[CC]   build/stax/obj/nbgl_obj_pool.o
[CC]   build/stax/obj/nbgl_page.o
[CC]   build/stax/obj/nbgl_screen.o
[CC]   build/stax/obj/nbgl_serialize.o
[CC]   build/stax/obj/nbgl_touch.o
[CC]   build/stax/obj/nbgl_use_case.o
[CC]   build/stax/obj/nfc.o
[CC]   build/stax/obj/os.o
[CC]   build/stax/obj/os_io_seproxyhal.o
[CC]   build/stax/obj/os_io_task.o
[CC]   build/stax/obj/os_io_usb.o
[CC]   build/stax/obj/os_printf.o
[CC]   build/stax/obj/osal.o
[CC]   build/stax/obj/parser.o
[CC]   build/stax/obj/parser_impl.o
[CC]   build/stax/obj/pic.o
```

© 2023 Nagravision Sàrl. All Rights Reserved

```
[CC]   build/stax/obj/qrcodegen.o
[CC]   build/stax/obj/secret.o
[CC]   build/stax/obj/segwit_addr.o
[CC]   build/stax/obj/sigutils.o
[CC]   build/stax/obj/stack_protector.o
[AS]   build/stax/obj/stack_protector_init.o
[AS]   build/stax/obj/svc_call.o
[AS]   build/stax/obj/svc_cx_call.o
[CC]   build/stax/obj/syscalls.o
[CC]   build/stax/obj/timeutils.o
[CC]   build/stax/obj/tx.o
[CC]   build/stax/obj/tx_display.o
[CC]   build/stax/obj/tx_parser.o
[CC]   build/stax/obj/tx_validate.o
[CC]   build/stax/obj/u2f_impl.o
[CC]   build/stax/obj/u2f_io.o
[CC]   build/stax/obj/usbd_ccid_cmd.o
[CC]   build/stax/obj/usbd_ccid_core.o
[CC]   build/stax/obj/usbd_ccid_if.o
[CC]   build/stax/obj/usbd_conf.o
[CC]   build/stax/obj/usbd_core.o
[CC]   build/stax/obj/usbd_ctlreq.o
[CC]   build/stax/obj/usbd_hid.o
[CC]   build/stax/obj/usbd_impl.o
[CC]   build/stax/obj/usbd_ioreq.o
[CC]   build/stax/obj/ux.o
[CC]   build/stax/obj/view.o
[CC]   build/stax/obj/view_nano.o
[CC]   build/stax/obj/view_s.o
[CC]   build/stax/obj/view_stax.o
[CC]   build/stax/obj/view_x.o
[CC]   build/stax/obj/zxformat.o
[CC]   build/stax/obj/zxmacros.o
[CC]   build/stax/obj/zxutils_ledger.o
[LINK] build/stax/bin/app.elf
[CP] build/stax/bin/app.elf => bin/app.elf
[CP] build/stax/bin/app.hex => bin/app.hex
[CP] build/stax/dbg/app.map => debug/app.map
[CP] build/stax/dbg/app.asm => debug/app.asm
[CP] build/stax/bin/app.apdu => bin/app.apdu
[CP] build/stax/bin/app.sha256 => bin/app.sha256
make[1]: Leaving directory '/app/app'
make[1]: Leaving directory '/home/joo/projects/zondax/app-cosmos-main'
```

B. CPP_TEST LOGS

```
USERID                      : 1000
GROUPID                     : 1000
TESTS_ZEMU_DIR              : /home/joo/projects/zondax/app-cosmos/tests_zemu
EXAMPLE_VUE_DIR             : /home/joo/projects/zondax/app-cosmos/example_vue
TESTS_JS_DIR                :
TESTS_JS_PACKAGE            :
mkdir -p build && cd build && cmake -DCMAKE_BUILD_TYPE=Debug .. && make
-- Conan: checking conan executable
-- Conan: Found program /home/joo/.local/bin/conan
-- Conan: Version found Conan version 1.59.0

-- Conan: Automatic detection of conan settings from cmake
-- Conan: Settings= -s;build_type=Debug;-s;compiler=clang;-
s;compiler.version=11;-s;compiler.libcxx=libstdc++11
-- Conan: checking conan executable
-- Conan: Found program /home/joo/.local/bin/conan
-- Conan: Version found Conan version 1.59.0

-- Conan executing: /home/joo/.local/bin/conan install
/home/joo/projects/zondax/app-cosmos/conanfile.txt -s build_type=Debug -s
compiler=clang -s compiler.version=11 -s compiler.libcxx=libstdc++11 -
g=cmake --build=missing
Configuration:
[settings]
arch=x86_64
arch_build=x86_64
build_type=Debug
compiler=clang
compiler.libcxx=libstdc++11
compiler.version=11
os=Linux
os_build=Linux
[options]
[build_requires]
[env]

...
test 1
    Start 1: unittests

1: Test command: /home/joo/projects/zondax/app-cosmos/build/bin/unittests
1: Test timeout computed to be: 10000000
1: Running main() from /home/joo/projects/zondax/app-
cosmos/build/googletest-src/googletest/src/gtest_main.cc
1: Number of testcases: 39
1: Number of testcases: 39
1: Number of testcases: 4
```

© 2023 Nagravision Sàrl. All Rights Reserved
Confidential

```
1: Number of testcases: 4
1: [==========] Running 140 tests from 6 test suites.
1: [----------] Global test environment set-up.
1: [----------] 2 tests from Address
...
1: [----------] 2 tests from Address (2 ms total)
1:
1: [----------] 14 tests from JsonParserTest
...
1: [----------] 14 tests from JsonParserTest (2 ms total)
1:
1: [----------] 33 tests from TxValidationTest
...
1: [----------] 33 tests from TxValidationTest (6 ms total)
1:
1: [----------] 5 tests from TxParse
...
1: [----------] 5 tests from TxParse (2 ms total)
1:
1: [----------] 78 tests from JsonTestCases/JsonTests_Secp256
...
1: [----------] 78 tests from JsonTestCases/JsonTests_Secp256 (65 ms
total)
1:
1: [----------] 8 tests from JsonTestTextualCases/JsonTests_Textual
...
1: [----------] 8 tests from JsonTestTextualCases/JsonTests_Textual (98 ms
total)
1:
1: [----------] Global test environment tear-down
1: [==========] 140 tests from 6 test suites ran. (179 ms total)
1: [  PASSED  ] 140 tests.
1/1 Test #1: unittests ........................   Passed    0.27 sec

100% tests passed, 0 tests failed out of 1

Total Test time (real) =   0.27 sec
```

C. CODEQL LOGS

```
"Include header files only","The #include pre-processor directive should
only be used to include header files.","recommendation","The #include pre-
processor directive should only be used to include header
files.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-
all.cc","46","1","46","23"
"Include header files only","The #include pre-processor directive should
only be used to include header files.","recommendation","The #include pre-
processor directive should only be used to include header
files.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-
all.cc","45","1","45","37"
"Include header files only","The #include pre-processor directive should
only be used to include header files.","recommendation","The #include pre-
processor directive should only be used to include header
files.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-
all.cc","44","1","44","32"
"Include header files only","The #include pre-processor directive should
only be used to include header files.","recommendation","The #include pre-
processor directive should only be used to include header
files.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-
all.cc","43","1","43","38"
"Include header files only","The #include pre-processor directive should
only be used to include header files.","recommendation","The #include pre-
processor directive should only be used to include header
files.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-
all.cc","42","1","42","37"
"Irregular enum initialization","In an enumerator list, the = construct
should not be used to explicitly initialize members other than the first,
unless all items are explicitly initialized. An exception is the pattern
to use the last element of an enumerator list to get the number of
possible values.","recommendation","In an enumerator list, the = construct
should not be used to explicitly initialize members other than the first,
unless all items are explicitly
initialized.","/deps/tinycbor/src/cbor.h","152","14","152","22"
"For loop variable changed in body","Numeric variables being used within a
for loop for iteration counting should not be modified in the body of the
loop. Reserve for loops for straightforward iterations, and use a while
loop instead for more complex cases.","recommendation","Loop counters
should not be modified in the body of the
[[""loop""|""relative:///_lgtm_build_dir/googletest-
src/googlemock/src/gmock.cc:150:36:175:3""]].","/_lgtm_build_dir/googletes
t-src/googlemock/src/gmock.cc","173","7","173","7"
"FIXME comment","Comments containing 'FIXME' indicate that the code has
known bugs.","recommendation","FIXME comment: The dispatch on
std::is_pointer was introduced as a workaround
for","/_lgtm_build_dir/googletest-src/googlemock/include/gmock/gmock-
matchers.h","2027","5","2027","80"
```

© 2023 Nagravision Sàrl. All Rights Reserved

```
"FIXME comment","Comments containing 'FIXME' indicate that the code has
known bugs.","recommendation","FIXME comment: Print the type of the leaked
object.","/_lgtm_build_dir/googletest-src/googlemock/src/gmock-spec-
builders.cc","625","7","625","52"
"FIXME comment","Comments containing 'FIXME' indicate that the code has
known bugs.","recommendation","FIXME comment: Validate attribute names are
legal and human readable.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/gtest.h","655","3","655","66"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-port.h","934","31","934","49"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/gtest-matchers.h","170","3","172","65"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-matchers.h","4760","1","4786","64"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-matchers.h","4619","1","4636","63"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-spec-builders.h","1939","1","1953","36"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-spec-builders.h","1864","1","1923","4"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/gtest-death-test.h","217","1","259","2"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/gtest.h","2356","1","2382","34"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/deps/tinycbor/src/cbor.h","126","1","126","55"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-actions.h","1168","1","1197","72"
"Commented-out code","Commented-out code makes the remaining code more
difficult to read.","recommendation","This comment appears to contain
```

```
commented-out code.","/_lgtm_build_dir/googletest-
src/googlemock/include/gmock/gmock-actions.h","381","3","383","34"
"Large object passed by value","An object larger than 64 bytes is passed
by value to a function. Passing large objects by value unnecessarily use
up scarce stack space, increase the cost of calling a function and can be
a security risk. Use a const pointer to the object
instead.","recommendation","This parameter of type
[[""RE""|""relative:///_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-port.h:893:18:893:19""]] is
144 bytes - consider passing a const pointer/reference
instead.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-death-test-
internal.h","169","29","169","33"
"Large object passed by value","An object larger than 64 bytes is passed
by value to a function. Passing large objects by value unnecessarily use
up scarce stack space, increase the cost of calling a function and can be
a security risk. Use a const pointer to the object
instead.","recommendation","This parameter of type
[[""ParamType""|""file:///:0:0:0:0""]] is 192 bytes - consider passing a
const pointer/reference instead.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-param-
util.h","438","48","438","56"
"Large object passed by value","An object larger than 64 bytes is passed
by value to a function. Passing large objects by value unnecessarily use
up scarce stack space, increase the cost of calling a function and can be
a security risk. Use a const pointer to the object
instead.","recommendation","This parameter of type
[[""ParamType""|""file:///:0:0:0:0""]] is 192 bytes - consider passing a
const pointer/reference instead.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-param-
util.h","397","47","397","55"
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable _ is never
read.","/_lgtm_build_dir/googletest-src/googlemock/include/gmock/gmock-
matchers.h","4063","33","4063","33"
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable kInternalRunDeathTestFlag is
never read.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-death-test-
internal.h","53","12","53","36"
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable kDeathTestUseFork is never
read.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-death-test-
internal.h","52","12","52","28"
```

```
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable kDeathTestStyleFlag is never
read.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-death-test-
internal.h","51","12","51","30"
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable kMaxStackTraceDepth is never
read.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/gtest.h","167","11","167","29"
"Unused static variable","A static variable that is never accessed may be
an indication that the code is incomplete or has a
typo.","recommendation","Static variable CborIndefiniteLength is never
read.","/deps/tinycbor/src/cbor.h","235","21","235","40"
"Inconsistent definition of copy constructor and assignment ('Rule of
Two')","Classes that have an explicit copy constructor or copy assignment
operator may behave inconsistently if they do not have
both.","warning","No matching copy assignment operator in class RE. It is
good practice to match a copy constructor with a copy assignment
operator.","/_lgtm_build_dir/googletest-
src/googletest/include/gtest/internal/gtest-port.h","897","3","897","4"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:118:28:118:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","118","9","118","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:118:46:118:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","118","9","118","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:123:28:123:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","123","9","123","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:123:46:123:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","123","9","123","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
```

```
address ([[""source""|""relative:///tests/tx_parse.cpp:62:28:62:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","62","9","62","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:62:46:62:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","62","9","62","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:72:28:72:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","72","9","72","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:72:46:72:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","72","9","72","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:79:28:79:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","79","9","79","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:79:46:79:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","79","9","79","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:88:28:88:30""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","88","9","88","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:88:46:88:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","88","9","88","48"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:97:28:97:30""]])
```

```
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","97","9","97","30"
"Local variable address stored in non-local memory","Storing the address
of a local variable in non-local memory can cause a dangling pointer bug
if the address is used after the function returns.","warning","A stack
address ([[""source""|""relative:///tests/tx_parse.cpp:97:46:97:48""]])
may be assigned to a non-local
variable.","/tests/tx_parse.cpp","97","9","97","48"
```

REFERENCES

© 2023 Nagravision Sàrl. All Rights Reserved
Confidential

DOCUMENT HISTORY

AUTHOR	STATUS	DATE	VERSION	COMMENTS
Joo Yeon Cho	Proposal	8 September 2023	V1.0	First version
Joo Yeon Cho	Proposal	19 September 2023	V1.1	Final version

REVIEWER	POSITION	DATE	VERSION	COMMENTS
Pascal Aubry	Senior Security Evaluations Lab Manager	8 September 2023	V1.0	
Gerrit Holtrup	Principal Security Engineer	8 September 2023	V1.0	
Gerrit Holtrup	Principal Security Engineer	19 September 2023	V1.1	

APPROVER	POSITION	DATE	VERSION	COMMENTS
Benoît Gerhard	Senior Director - Security Evaluations Lab	8 September 2023	V1.0	
		Select the Date		
		Select the Date		

© 2023 Nagravision Sàrl. All Rights Reserved