The Quantum Resistant Ledger

X41 Audit: Response

September/October 2018

Foreword

The QRL developers would like to thank X41 D-Sec GmbH and Secfault Security GmbH for their professionalism in completing their review of the Quantum Resistant Ledger.

Working closely with our team with exceptional communication throughout the review process has allowed a rapid implementation of fixes for issues raised and improvements in development strategies.

An abbreviated summary of discussion points raised in the report and actions taken follows.

The QRL Core Developers

Critical

N/A

High

QRL-PT-18-03

OTS Indices out of Sync

Status: FIXED

The OTS key is written to disk before the broadcast of the transaction is initiated.

QRL-PT-18-05

qrllib / Signature Stack Allocation Overflow

Status: FIXED

Although the clients provide protection against exploitation, as a library QRLLIB has the potential to be used in other products. The reference code used in QRLLIB has been patched to use a safe memory allocator and the issue in the reference code has been reported in case of any impact on other implementations.

Medium

QRL-PT-18-00

External Proto Files

Status: FIXED

Hashes of valid proto files are now used in the web wallet, as per the description in the report.

QRL-PT-18-01

Missing Key Derivation

Status: ROADMAP (v2 wallet)

AES in GMC mode has been added to the roadmap to strengthen the encryption of wallet files.

QRL-PT-18-02

Use of Non-Authenticated Encryption

Status: ROADMAP (v2 wallet)

Use of scrypt has been added to the roadmap to improve the treatment of passphrases.

Low

QRL-PT-18-04

Non-Atomic Filesystem Interaction

Status: MITIGATED

As per the report, this is non-trivial and solutions are platform specific. Confirmation of OTS key index from the chain mitigates this risk.

None

QRL-PT-18-100

Shift of Signed Values - Undefined Behaviour

Unused code.

QRL-PT-18-101

QRL Generate Tool - Code Injection

Only used to generate a genesis block. Fixed in PR#1585 in case of use in an alternative deployment of the QRL.

QRL-PT-18-102

Tree Height Truncation in qrllib / XMSS interface

Although the likelihood of this ever being an issue is remote, it has been fixed in #156.

QRL-PT-18-103

Unorthodox Seed Generation Method

This is limited by the hardware used as we agree the entropy is sufficient.

QRL-PT-18-104

Potential Key Collisions in State Handling

Solution as suggested added to roadmap (low priority) with an additional safeguard of additional validation to verify data related to the hash in state and rejection of block/transaction as necessary.

QRL-PT-18-105

Truncation For Inputs Larger 4GB

Suggested solution implemented.

theqrl.org