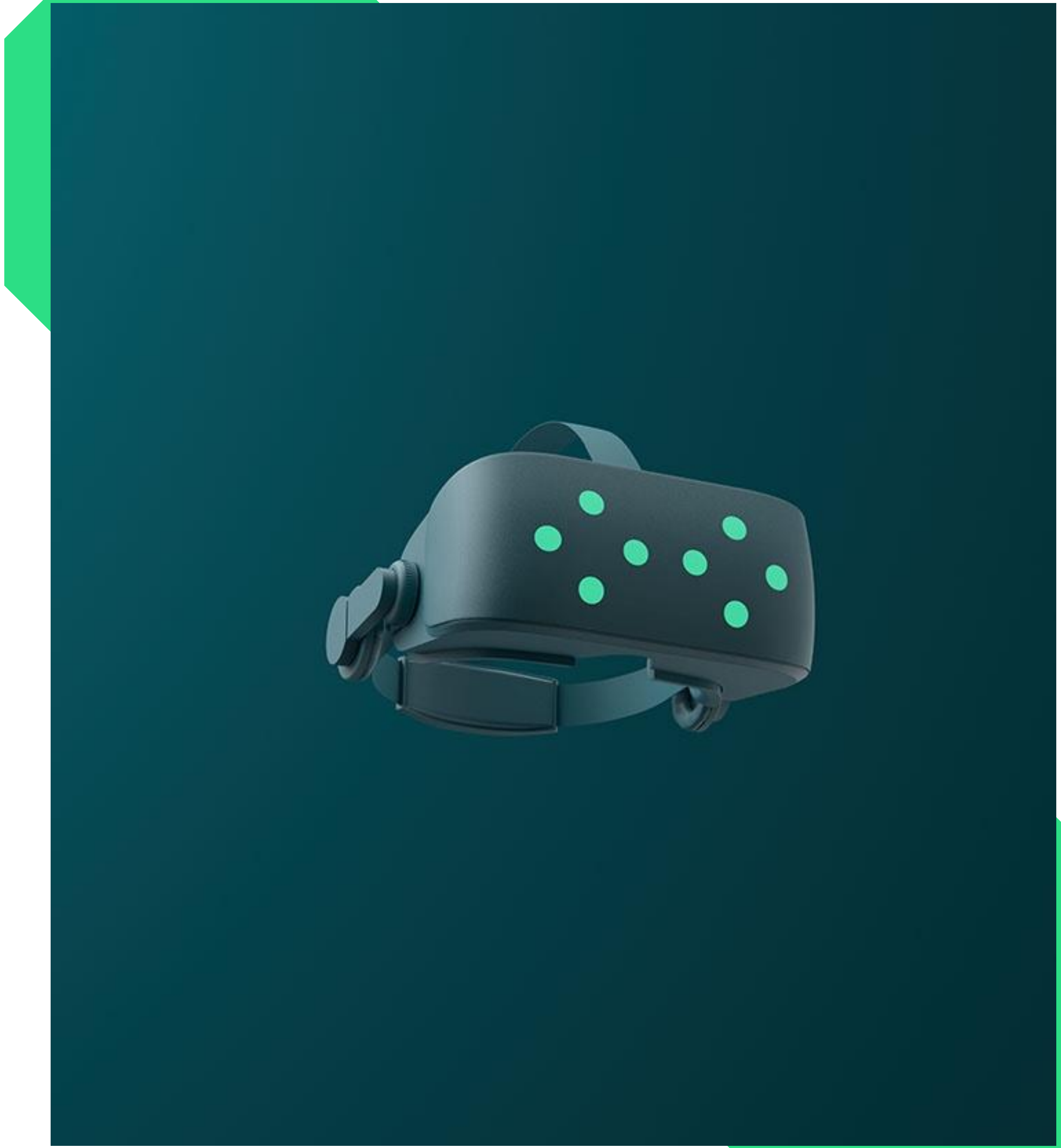
The Cyber Resilience Act and Me

… as a contributor to Qt

August 2024

Qt Development



The attack surface of Qt

- … is a subset of the attack surface of any Qt application
- … is largely defined by how malicious input can be injected into the Qt process
  - to exploit bugs that might result in arbitrary code execution (e.g. through stack corruption)
  - circumvent existing security protocols
  - elevate privileges

Malicious Data

For now, we are focusing on those parts of Qt that process data that, by design, can not be controled by the application.

Such as…

- Files loaded by the user
- Network traffic received
- Content pasted from the clipboard
- Images decoded as part of a document

We want to identify code in Qt that participates in the processing of untrusted, potentially malicious data

- Network protocol stack
  - Esp anything related to data encryption/decryption
- Parsers and decoders
  - Image format handlers
  - Text decoders
  - String parsers

- Note: some functionality in Qt is explicitly not designed to handle data from untrusted sources.
  - QDataStream
  - QML Engine

Extra scrutiny for changes to such code

- Make reviewers aware of the nature of the change
- Require extra reviews
- Run fuzz-tests, static analysis, code coverage measurements

- Proposal: tagging source files using a source code comment
  - https://codereview.qt-project.org/c/meta/quips/+/575276
  - Once agreed, implement Gerrit support to highlight such changes and evaluate automation options

```
// Qt-Security score:significant reason:data-parser
// Qt-Security score:critical reason:cryptography
```

Gerrit Account Life-Cycle

- Gerrit Accounts never expire or get deactivated after inactivity
- Approver privileges are never removed
- Bad combination

- Governance model provides mechanism to remove Maintainer responsibility/privilege from inactive users
  - As per https://lists.qt-project.org/pipermail/development/2022-September/042922.html
- Nothing equivalent in place for Approver privileges, or accounts deactivation

Proposal

After sufficiently long inactivity

1. Automatically lock gerrit account
   - After X months of inactivity
   - Self-service reactivation via email verification roundtrip (e.g. same as creating a new account)
2. Automatically remove approver privilege
   - After X months of inactivity: Can be reactivated by request to gerrit-admin
   - After Y months of inactivity: Requires new nomination

X = 6 months

Y = 12 months