IOHK

Mitigation Verification

April 2020

Published April 21, 2020

CONFIDENTIAL INFORMATION ENCLOSED

On April 20, 2020, IOHK released “Response to Security Audit Report (Byron Reboot)” listing remediation steps and/or mitigating clarifications to the identified areas of concern in the Phase 1 and Phase 2 audit reports.

root9B (R9B) reviews those responses by issue below.

1. Insecure Genesis Key Generation.
   IOHK has both verified the code in question was used only for test and Quality and Assurance (QA) purposes and not for production keys, as well as altered the code to use secure key generation. R9B confirms these steps fully address Issue 1.

2. Code Practice – ReadFile.
   R9B confirms IOHK changes fully address Issue 2.

3. Code Practice and Potential Resource Usage – Async Read.
   R9B confirms the changes fully address Issue 3.

4. Potential Resource Usage/Denial of Service (DoS).
   R9B confirms the changes fully address Issue 4.

5. Potential Protocol Incompletion – Static Node Set.
   IOHK has clarified that this code is only for testing. R9B accepts this resolution.

6. Primitive Usage – Mock Crypto.
   IOHK has confirmed the mock implementations are not for production use, with real implementations forthcoming. R9B accepts this resolution.

7. Weakened Protections – CSP in Electron App Daedalus.
   IOHK identified a valid requirement to use this CSP configuration until Chrome can evaluate WASM without it. As this is not a vulnerability, R9B accepts this resolution.

8. Blake Hash Function Only Performed Once When Applying a Spending Password.
   IOHK confirms the Daedalus frontend to Cardano wallet backend connection relies on TLS for password security in transmission and plans to phase out Blake hashing. R9B accepts this resolution.

9. Address Randomization Suggestion.
   IOHK confirms address randomization is for port conflict avoidance. R9B accepts this resolution.

10. Potential Future Issue - Payment URI.
    IOHK plans to heed this potential area of concern for code that may encounter it. R9B accepts this resolution.

11. Theoretical Denial of Service (DoS) Vulnerability.
    As mentioned in the Phase 1 Report (published January 31, 2020) and referenced in the "Response to Security Audit Report (Byron Reboot)," the Ouroborous Praos private slot-leader schedule (Shelley) will fully resolve this issue.

12. Update Process.
    IOHK explained plans to replace this update process with a new one to be released in April 2020. R9B accepts this resolution.

13. IOHK Monitoring Web Frontend Exposure.
    IOHK has removed exposed surface, including disabling the frontend in question in configuration. R9B accepts this resolution.