G_0 Group

Security Review of

Tangem Payment Processor

August 2022

Tangem Payment Processor / August 2022

Files in scope

Following solidity files:

https://github.com/gnosis/TangemPaymentProcessor/blob/255656a2e367af5f05eb6fc6e4ce341ad4705da3/contracts/OTPProcessorSingleUser.sol
https://github.com/gnosis/TangemPaymentProcessor/blob/255656a2e367af5f05eb6fc6e4ce341ad4705da3/contracts/OTPProcessorMultiUser.sol

Current status

All discovered issues have been fixed by the developer. There are no known issues in the relevant contracts in
https://github.com/gnosis/TangemPaymentProcessor/tree/6d2b9a9217c19d74aa58466d297ad0a9553ac912/contracts

Issues

1. otpRootCounter is not updated

type: incorrect implementation / severity: critical

In both `OTPProcessorSingleUser.process` and `OTPProcessorMultiUser.process`, `otpRootCounter` is not updated after processing transactions, this allows the same transaction to be processed repeatedly.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/TangemPaymentProcessor/tree/6d2b9a9217c19d74aa58466d297ad0a9553ac912/contracts

2. Wrong condition for preventing re-submittal of historic transactions

type: incorrect implementation / severity: critical

On lines
https://github.com/gnosis/TangemPaymentProcessor/blob/255656a2e367af5f05eb6fc6e4ce341ad4705da3/contracts/OTPProcessorSingleUser.sol#L102
and
https://github.com/gnosis/TangemPaymentProcessor/blob/255656a2e367af5f05eb6fc6e4ce341ad4705da3/contracts/OTPProcessorMultiUser.sol#L112
the condition should use `<=` opeator instead of `<`, otherwise last transaction can be resubmitted repeatedly.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/gnosis/TangemPaymentProcessor/tree/6d2b9a9217c19d74aa58466d297ad0a9553ac912/contracts