20 MATTER SECURITY PITFALLS

DEVELOPERS SHOULD CONSIDER

01 Implementing a weak random number generator

02 Insufficient protection of the device passcode

03 Insecure implementation of the multi-admin and multi-fabrics feature

04 Failure to achieve unique identifiers

05 Risking access control list wildcards and inconsistencies

06 Risks specific to bridges and bridged devices

07 Risking privacy by advertising vendor and product identifiers via DNS or Bluetooth

08 Risks specific to controllers, commissioners, edge routers, bridges, OTA providers and OTA requestors

09 Unsanitized user input

10 Rogue commissioners

11 Devices may ignore device attestation verification results

12 Evil twin attack

13 Manipulation of the CommissioningCustomFlowUrl

14 HTTP downgrade attack

15 Missing minimal requirements for underlying communication channels

16 Manipulation of sleepy end device parameters

17 Status report message injection

18 Revocation from groups

19 Underspecification of timed interactions

20 Dysfunctional implementations of event logging

See our blog post for recommendations on how to avoid them: schutzwerk.com/blog/matter-security-considerations

SCHUTZWERK