Credential Cloning.

Severity: High

Components affected: ICT factory default MIFARE and DESFire cards and tags/fobs

Reported by: Thomas Hobson

Active exploitation of vulnerability*: No

Description of vulnerability: Insecure storage of the ICT MIFARE and DESFire encryption keys in the firmware binary allows malicious actors to create credentials for any site code and card number that is using the default ICT encryption.

Mitigation:

Any place and vertical can benefit from a robust unified access control and security solution, including:

- We recommend setting up two-factor-authentication (2FA) on all doors where PIN readers are installed to mitigate the risk of using credentials with publicly available default keysets
- Use custom keysets unique to customer sites to prevent cards being created by third parties using exploited publicly available default keysets

To set up 2FA, please refer to:

- Protege GX Operator Reference Manual
- Protege WX Programming Reference Manual

To set up custom keysets, please refer to Application Note AN-352: Setting Up Custom Credential Encryption

*This indicates whether ICT is aware of this being actively exploited against customer sites at the time of publication.