NCR ATM Security Update

DATE: January 18, 2021 **INCIDENT NO:** 2021-01 **REV:** #1

Man in the Middle Logical Attacks in India

New guidance and recommendations from NCR

NCR has been made aware of two Man in the Middle logical attacks in India, both of which resulted in cash losses. One attack was against an NCR ATM, the other was against another brand from a different vendor.

In both cases an ATM was located in an ATM room adjacent to a bank branch. The ATM was connected to the financial network via a network cable from the ATM to a wall socket connected to the bank branch. This network cable in the ATM room was physically accessible to the attacker, and there was no logical protection on the communications between the ATM and the wall socket.

A network router, with capability to modify the responses back from the Authorisation Host, was connected in line with this cable.

The attacker then used a known blocked card to submit a withdrawal request. When the host responded with a message declining the transaction, the Man in the Middle changed that response to approve the transaction, allowing the attacker to withdraw cash from the ATM without approval, or a corresponding debit to the account.

NCR Recommendations

- Follow industry best practice for securing TCPIP networks.
- Standard communications authentication and encryption protection must be applied to all ATM network traffic. The recommendation is to use a minimum of TLS 1.2 or a VPN. It is critical that the encryption is applied strictly end to end, that is, from the ATM PC core all the way to the host.
- Implement MAC'ing to provide cryptographic authentication of sensitive messages.
- NCR would also recommend that network cables should not be located in publicly accessible locations, or network cables should be physically protected.

Contacts

ATM Crime Reporting: Global.Security@ncr.com

Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com