NCR SECURITY UPDATE

DATE: January 25, 2019 **INCIDENT NO:** 2019-MX1 **REV:** 1

Black Box attacks on 6622 model ATMs in Mexico

Summary

NCR has received reports of several successful “Black Box” attacks on NCR SelfServ 6622 model ATMs in Mexico. The ATMs attacked were using dispenser component software USBCDM 03.07.00 and USBCDM 04.01.01, and NCR has confirmation that at least one of the ATMs was correctly configured with the previously recommended settings to prevent Black Box attacks.

At this time, NCR’s view is that criminals have further developed endoscope techniques which they are using to manipulate electronic sensors on the dispenser within the ATM safe, with the goal of simulating actions which are designed only to be performed if the safe door is open. These actions authorize the dispenser firmware to cryptographically re-authenticate to the Black Box, which facilitates the attack.

The authorization mechanism which causes the dispenser firmware to cryptographically re-authenticate, that is implemented in USBCDM 03.07.00 and USBCDM 04.01.01 software, requires that the dispenser is racked out, manipulation of the bottom cassette, and a toggle of the switch on the control board. NCR now believes that these actions can be simulated with an endoscope, and may involve unlatching of cassettes and removal/replacement of connectors on the control board. The exact attack mechanism is still to be confirmed.

NCR immediate actions

NCR intends to issue an emergency software / firmware update to all Mexico customers as soon as possible. This will be in the form of an APTRA XFS USB Currency Dispenser component. This component will contain new firmware, and it will have the dependencies that component versions USBCDM 03.07.00 or USBCDM 04.01.01 are already installed. These dependencies will allow the size of the new component will be kept to a minimum.

The functionality of the new firmware will be to provide a new authentication sequence which will be far more difficult to simulate. This is described in the next paragraph.

This emergency component will have a fixed configuration, i.e. there will be no options to change the dispenser protection level, or the dispenser configuration sequence.

The emergency component will not contain any updates to SYSAPP. This means that the new authentication sequence will not be described on the ATM service panel. Any authorized service engineer will require to have this communication in order to know the correct authentication sequence. NCR has decided not to make any SYSAPP changes for the emergency component to ensure that the component can be delivered in the shortest possible time. It will also help to mask the presence of the new functionality from an attacker.

The absence of SYSAPP changes will mean that the configuration options for dispenser protection level and dispenser authentication sequence will appear to be present and working, but the firmware does not support configuration options and therefore nothing will change at the firmware level. This is important for laboratory testing and evaluation, where it may appear that the protection can be downgraded.

Authentication Sequence Description

The previous dispenser components offered a choice of 3 authentication sequences. The emergency component will offer only one, called ‘cassette swap’. This authentication sequence is as follows:

1. Rack out dispenser
2. Remove the bottom cassette and remove the top cassette. When the second cassette is removed, a 50 second timer will commence, and all other authentication actions must complete before this timer expires. If the timer expires, replace the cassettes and restart the sequence.
3. Replace the bottom cassette in the top position and replace the top cassette in the bottom position. i.e. swap the position of the cassettes.
4. Remove the top and bottom cassettes and replace them back in their original positions.
5. Toggle the control board switch, flick it one way, then return it to its original position.
6. Rack in the dispenser.

Authentication Sequence Dependencies

For this sequence to operate, the top cassette and the bottom cassette cannot be the same cassette type i.e. they must contain different currency denominations.

For lab testing, if it is necessary to roll back the firmware to a previous version, then the ‘cassette swap’ sequence must be performed to allow the firmware to roll back.

If Diagnostic Dispense is enabled, then the ‘cassette swap’ sequence must be performed to allow the action. NCR strongly recommends that Diagnostic Dispense is disabled in Mexico. Set registry parameter ‘DDD’ = 1 to disable this function.

Recommendations

- Update all 6622 ATMs in Mexico with the emergency dispenser component as soon as possible. This component will be provided to NCR Mexico Professional Services by 25th January 2019. Mexico financial institutions will receive the new software from their NCR Professional Services representative.
- Disable Diagnostic Dispense capability.

NCR follow up actions

The intent of the emergency component is to stop the current occurrences of black box crime in Mexico as soon as possible. This component is not intended as a global release due to the dependencies which will limit its applicability to other global environments. This software will therefore only be provided to Mexico.

Following successful deployment of the emergency component, NCR will begin development of a new dispenser component for new global release which will have either the same or improved security properties over the emergency component. The global release will replace the emergency component and will represent the supported NCR solution for Black Box attacks on S1 currency dispensers. The emergency component will be supported on an as required basis, until such time as the global release is available.

NCR does not have a committed schedule, or finalized specification, for the global release at this time. It is expected that the global release will be available within 3-6 months of the date of this communication.