NCR ATM SECURITY UPDATE

DATE: February 6, 2018 **INCIDENT NO:** 2018-04 **REV:** #1

Critical Platform Component Update for S1 and S2 Currency Dispenser

Summary

NCR is releasing a critical platform firmware component update for both the S1 and the S2 dispenser. This update contains two very important changes designed for greater protection against Black Box attacks.

1. The physical authentication mechanism used to authorize encrypted communications to the dispenser has been strengthened to add protection against an attacker using endoscope technology in an attempt to manipulate dispenser electronics from outside the safe. Additionally, further authentication mechanisms have been added as configuration options.
2. A vulnerability in the anti-roll back protection has been addressed.

NCR's long-standing recommendation has been to configure NCR ATM Currency Dispensers to Level 3 Protection. For all NCR customers who have configured Level 3 Protection as a protection against Black Box attacks on S1 and S2 dispensers, this firmware upgrade is required to support that protection. Customers should plan to deploy this update as soon as possible.

Reference NCR Security Alert Incident No. 2017-09

Additional recommendations for taking full advantage of security features in S2 Currency Dispensers is included at the end of this alert.

NCR ATM SECURITY UPDATE

Release Description:

For protection against Endoscope attacks, two changes have been made to the S1 and S2 firmware.

1. The authentication sequence mechanism for detection of cassette removal has been strengthened such that it is unlikely for an attacker to successfully simulate cassette removal using an external magnet near the sensor.
2. Additional authentication sequence options have been added to provide higher security mechanisms. These configurable options are to provide additional protection should the attack technique evolve beyond simple endoscope attacks.

Authentication Sequence Options for **Level 3** Dispenser Protection:

S1: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBCurrencyDispenser/Operational Parameters Dispenser Authentication Level	
Sequence 1 (Default)	Remove bottom cassette **OR** Insert bottom cassette **OR** Toggle switch on control board Action must complete within 60 seconds of command
Sequence 2 (Minimum Recommended Level)	Remove bottom cassette **AND** insert bottom cassette, **THEN** remove purge bin **AND** insert purge bin Full sequence must complete within 20 seconds
Sequence 3	(Rack out dispenser **AND** Remove bottom cassette **AND** Insert bottom cassette **AND** Toggle switch on control board **AND** Toggle switch back again **AND** Rack in dispenser) Sequence must complete within 20 seconds

NCR ATM SECURITY UPDATE

S2: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBMediaDispenser/Operational Parameters Dispenser Enable Level	
Sequence 1 (Default, Recommended)	Remove bottom cassette **AND** insert bottom cassette only Action must complete within 60 seconds of command, cassette must be replaced with 10 seconds of removal
Sequence 2	Remove bottom cassette **AND** insert bottom cassette, **THEN** remove purge bin **AND** insert purge bin Action must complete within 60 seconds of command, sequence must complete within 20 seconds

The authentication sequence only applies to Currency Dispensers set to Level 3 Protection; this firmware update will not provide further protection unless Level 3 Protection is configured. Any Currency Dispenser not set to Level 3 Protection should be understood as vulnerable to Black Box attack.

The authentication sequence level can be *increased* remotely. The authentication sequence can be *decreased* only if the current authentication sequence is performed. (e.g. to move an S2 Currency Dispenser from Sequence 2 to Sequence 1, it will be necessary to remove and insert the bottom cassette, then remove and insert the purge bin, within one minute after issuing the command.)

For the S1 Currency Dispenser, Sequence 2 is the **MINIMUM RECOMMENDED OPTION**, and this setting **MUST** be configured when the software is deployed.

NCR ATM SECURITY UPDATE

Anti-rollback protection is a critical feature included in the Level 3 Dispenser Protection mechanism. Firmware roll back is not restricted for S1 or S2 Currency Dispensers set to Protection Level 1 or Level 2. This firmware release includes updates to address a vulnerability in the roll back prevention mechanism in the Level 3 Dispenser Protection.

Applicability:

This critical update is for a mechanism in Level 3 Protection for S1 and S2 Currency Dispensers. The update is compatible with all supported APTRA XFS versions (currently APTRA XFS 06.03.01 and later).

Release Version:

This firmware update to the S1 and S2 Currency Dispensers is released as an APTRA XFS platform update package.

APTRA XFS Module and Security Update Package 01.00.00

The respective versions are:

- S1: USBCurrencyDispenser 03.07.00, firmware 0x0156
- S2: USBMediaDispenser 02.05.00, firmware 0x0108

How to obtain this software:

This critical firmware update is available on the Software Download Centre from February 7th, 2018. It will also be included in the next APTRA XFS platform release, APTRA XFS 06.06. NCR Channel Partners should go through normal software release channels.

References:

Security is Not an Option White Paper: Dispenser Security Solution

APTRA XFS Module and Security Update Package 01.00.00 Release Notes

NCR ATM SECURITY UPDATE

S2 General Security Guidance and Recommendations:

In addition to Black Box protections, the S2 dispenser also supports a number of additional configuration options which can be used to deter and detect other forms of crime. NCR recommended settings are as follows:

Function	Purpose	Description
Programable pre-present	To prevent forms of Transaction Reversal Fraud e.g. by malicious card fault or shutter fault	Carriage can be programmed to remain at the rear of the dispenser, prior to shutter opening.
Programable Park	To prevent access into the safe for the purpose of introducing explosive material (gas or solid)	The S2 note carriage can be programmed to lock in position blocking access through the dispenser transport into the safe
Programable Park	To prevent possibility of reject bin fishing on front access ATMs	The S2 note carriage can be programmed to lock in position blocking access to the reject bin
Carriage Sweep	To detect the insertion of type 2 cash traps	The S2 carriage can be programmed to 'sweep' along the transport, prior to cash loading. This action will trigger a type 2 cash trap without exposing any currency
Diagnostic Dispense Authentication	To prevent misuse of diagnostic capabilities	All diagnostic commands that move currency can be disabled unless authorization is demonstrated

NCR ATM SECURITY UPDATE

Tamper Sensors	To detect anomalous behavior indicative of tampering, TRF, fishing	S2 sensors can be enabled to detect suspicious behavior, within the context of a transaction, and during idle time. Alert status can be sent to the application. S2 can be configured to automatically go out of service on detection of an alert.
Prepare for dispense	To offset any increase in transaction time	Programable Park can add 2 seconds to transaction time. This can be offset by an application modification to issue 'prepare for dispense'.

For more detail on these settings, please see APTRA XFS release notes.

Customers who would like to get additional guidance as to their current state of security deployment and how it aligns with NCRs best practices are encouraged to sign up for the **ATM Security Assessment.**

Please contact your NCR Account Manager if you have any questions or need additional information.

Links

Security Alerts Archive

February 14, 2018 Webinar: Protecting your ATMs from Malware and Black Box Attacks

NCR ATM SECURITY UPDATE

Contacts

ATM Crime Reporting : global.security@ncr.com
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com
Further information on this alert please contact Owen Wild
Please refer any media inquiries or questions to Aaron Gould