NCR SECURITY ADVISORY

DATE: March 5, 2021 **REV:** 4

NOTE: This information is time sensitive. Check with your NCR representative for later versions of this advisory.

Configuration advisory for S1 and S2 Currency Dispenser to prevent "Black Box" and Diagnostic Misuse attacks

Summary

"Black Box" attacks are defined as an attack where the currency dispenser is disconnected from the ATM PC Core, and reconnected to the attackers' device (e.g. laptop, mobile phone, raspberry pi etc). The attackers' device then communicates with the dispenser, and overcomes the cryptographic protection through reset of the cryptographic keys, or by firmware manipulation. A second MO is also possible through misuse of diagnostic commands. This advisory documents NCR's instruction on how to configure the S1 and S2 dispenser to prevent such attacks.

This advisory version lists an additional Dispenser Authentication Sequence for S1 which should be used on High Risk ATMs. High risk ATMs with S1 dispenser should be upgraded with this software component and this new Authentication Sequence should be configured.

NCR SECURITY ADVISORY

Firmware:

The latest versions of firmware are released in platforms **XFS 06.08.00 and XFS for Windows 10 01.04**

This contains:

- S1: USBCurrencyDispenser 04.05.00, firmware 0x0193
- S2: USBMediaDispenser 03.10.00, firmware 0x0138

Configuration:

There are two critical parameters which **MUST** be configured correctly. These are

- Dispenser Protection Level
- Dispenser Authentication Sequence

NCR SECURITY ADVISORY

Dispenser Protection

Protection Level S1 / S2	Authentication Function
xxxx-F325 / F625 Level 1 USB Protection **Does not protect against Black Box**	Level 1 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software
xxxx-F326 / F626 Level 2 Logical Protection **Does not protect against Black Box**	Level 2 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software, and that a valid NCR USB Service Dongle is presented to the PC Core.
xxxx-F327 / F627 Level 3 Physical Protection **Mandatory level to protect against Black Box attacks.**	Level 3 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software, and that safe access is demonstrated by performing the appropriate authentication sequence.

For S1 and S2, Dispenser Protection Level 3 **MUST** be set. This configuration should be applied at the factory, and can be specified by order of feature F327 (S1) and F627 (S2).

NCR SECURITY ADVISORY

Authentication Sequence

S1 Dispenser:

S1: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBCurrencyDispenser/Operational Parameters/Dispense Authentication Level	
Sequence 1: dword:00000000 (Default – does not protect against some forms of Black Box attack)	Remove bottom cassette **OR** Insert bottom cassette **OR** Toggle switch on control board Action must complete within 60 seconds of command
Sequence 2: dword:00000001 (Min. 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: dword:00000002	(Rack out dispenser **THEN** Remove bottom cassette **AND** insert bottom cassette **THEN** Toggle switch on control board **AND** Toggle switch back again **THEN** Rack in dispenser) Sequence must complete within 20 seconds
Sequence 4: dword:00000003 (Note: for sequence 4 to be effective the top and bottom cassettes must have a different currency configuration such that the firmware can recognize the cassette swap)	(Rack out dispenser **THEN** Remove bottom cassette AND remove top cassette **THEN** Replace bottom cassette in top position **AND** Replace top cassette in bottom position **THEN** Return bottom and top cassettes to original positions **THEN** Toggle switch on control board **AND t**oggle switch back again **THEN** Rack in dispenser) Sequence must complete within 40 seconds

NCR SECURITY ADVISORY

For the S1 Currency Dispenser, Sequence 2 is the **MINIMUM** recommended option, and this setting **MUST** be configured when the software is deployed. **Sequence 4 SHOULD be used in high risk locations or high risk ATM models**.
High risk locations include Mexico; High risk ATM models include 6625.

S2 Dispenser:

S2: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBMediaDispenser/Operational Parameters/Dispense Enable Level	
Sequence 1: dword:00000001 (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: dword:00000002 Note: Available in APTRA XFS 6.06 and above only	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

For the S2 Currency Dispenser, Sequence 1 is the **MINIMUM** recommended option, and this setting is the default. Sequence 2 **SHOULD** be used in high risk locations.
High risk locations include Mexico.

NCR SECURITY ADVISORY

Additional Protection:

Further parameters are available which can be applied to provide additional protection to the dispenser. NCR recommends that these are set, unless there are strong business reasons for not doing so.

- Set 'Disable DPL Runtime Config' =dword:00000001

This removes the option to change configuration settings from SYSAPP.

- Set 'DDD' =dword:00000001

This disables the diagnostic dispense function (only for S1 dispensers).

Summary:

1. Deploy the latest version of Dispenser Platform Software. NCR apply critical security patches to the dispenser platform software, and it is imperative that customers maintain their platform software to the latest version. The minimum version which must be used is APTRA XFS Dispenser Security Update 01.00.00

2. Set the Dispenser Protection Authentication level to Level 3, Physical Protection.

3. For S1 dispensers, set the Dispenser Authentication Sequence to Level 2 (Dispense Authentication Level = dword:00000001)

4. For high risk locations e.g. Mexico, or for high risk ATM models, set the S1 Dispenser Authentication Sequence to Level 4 (Dispense Authentication Level = dword:00000003)

5. Apply additional layers of protection e.g. disable diagnostic dispense (for S1), disable SYSAPP configuration of settings.

Anything less will NOT protect the ATM against Black Box Attacks.

NCR SECURITY ADVISORY

Applicability:

This advisory is applicable to all S1 and S2 currency dispensers. The minimum firmware is compatible with all supported APTRA XFS versions (currently **XFS 06.05.00** and later).

How to obtain the firmware:

The firmware update is available in the latest released NCR platform software. Firmware is packaged with the corresponding drivers as platform software components for the S1 and the S2. Firmware is therefore deployed by installing the platform components. This can be done either by a complete upgrade of the NCR platform software or by integrating the new software components into an existing supported platform. NCR Professional Services can assist with platform or platform component upgrades. Please contact your NCR representative for further information. NCR Channel Partners should go through normal software release channels.

NCR SECURITY ADVISORY

SUPPLEMENTARY INFORMATION

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 prepresent "Pre-present enabled"	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 "Idle Position"	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 "Idle Position"	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 "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

NCR SECURITY ADVISORY

Diagnostic Dispense Authentication "Dispense Enable Level"	To prevent misuse of diagnostic capabilities	All diagnostic commands that move currency can be disabled unless authorization is demonstrated
Tamper Sensors "Tamper Security Level" and "Tamper Recovery Procedure"	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 Application Command	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 online help.

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

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