NCR ATM Security Update

DATE: July 8, 2021 **INCIDENT NO:** 2021-04 **REV:** #1

Press reports of NFC flaws at ATMs

Guidance and recommendations from NCR

NCR is aware of recent press reports of a security study of NFC (Near Field Communications) technology used in the ATM and payment industries that suggested that ATMs with this NFC technology could be vulnerable to hacking "by waving a phone." The report covers underlying research into the security of embedded contactless systems including those of the vendor that supplies devices for use in NCR ATMs.

The serious potential impacts identified in the reports could occur (i.e., would be possible) only if there were additional, yet undiscovered, vulnerabilities elsewhere in the system. **Regardless, NCR recommends that customers apply the software update below to remove this specific vulnerability with the Contactless Card Reader (CCR).**

NCR has been supplied new firmware by the CCR vendor to NCR which removes the vulnerability. **NCR customers should treat this update as IMPORTANT and apply at the earliest opportunity.**

In January 2021 (W10 platform) and March 2021 (W7 platform), NCR released platform software updates for the CCR model name **Kiosk III** used in NCR ATMs that contains the new firmware. This software is released as a component for both the Windows 7 and Windows 10 platform systems.

Software update details

- Component **USBContactlessCardReader2 02.04.00**
- Released in **XFS for Windows 10 01.04** and **XFS 06.08.00**

Note: The current model of CCR supported on NCR ATMs is the Kiosk III. The first version of CCR supported by NCR, Kiosk II, was discontinued in 2017. A component update for the Kiosk II CCR is

pending following scheduled delivery of firmware to NCR. An announcement on Kiosk II software component update will follow shortly.

NCR recommendations

All ATMs with Kiosk III CCRs that have not deployed USBContactlessCardReader2 02.04.00 should install and run the new component software at the earliest opportunity consistent with customer patching schedules.

All customers should be aware of, and should follow, ATM logical security guidance from NCR. This guidance can be found in the NCR Logical Attacks Whitepaper and lists 15 rules for the full protection of ATMs. All rules should be followed including the following rules, which help mitigate against new vulnerabilities found in deployed software:

- Rule 6: Deploy an effective anti-malware mechanism, specifically an active whitelisting application.
- Rule 7: Establish a regular patching process for all software installed.
- Rule 8: Harden the Operating System.

For more information on how to obtain the new component and upgrade, contact your NCR support channel.

Contacts

- ATM Crime Reporting: Global.Security@ncr.com
- Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com

Best regards,

NCR Banking Team