NCR ATM Security Update

DATE: October 5, 2021 **INCIDENT NO:** 2021-04 **REV:** #2

As communicated on July 8th 2021 in revision #1 of this alert, press reports of a security study of NFC (Near Field Communications) technology used in the ATM and payment industries suggested that ATMs with this NFC technology could be vulnerable to hacking "by waving a phone." The press report covered 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).**

The CCR vendor supplied new firmware to NCR that removes the vulnerability.

NCR customers should treat this update as IMPORTANT and apply at the earliest opportunity.

NCR have deployed two different contactless devices, named "**Kiosk II**" and "**Kiosk III**".

In January 2021 (for W10 platform) and March 2021 (for W7 platform), NCR released platform software updates for the CCR model named **Kiosk III**. The **Software update details were as follows:**

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

IMPORTANT: The prior version of CCR supported by NCR, named **Kiosk II (**discontinued in 2017), now has a component update available under version **USBCCR_95020102.** This is available through your NCR support channels.

NCR recommendations

All ATMs with Kiosk II and Kiosk III CCRs that have not deployed the new software updates should install and run these new components 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 with an emphasis on 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

NCR Corporation 864 Spring St. NW, Atlanta, GA 30308-1007