Serianu Cyber Security Advisory

2020 ATM Attacks Advisory for Banks

Serianu SOC Advisory Number:

TA – 2020/0012

Date(s) issued:

15th September 2020

Systems Affected:

- ATMs

Overview:

ATMs have long been a target for criminals and many traditional attacks focused on physically breaking into the cash safes where money is stored within the ATM. However, over the past decade, criminals have progressed to logic-based attacks that trick machines into dispensing cash. These attacks can involve malware, network-based attacks or directly attaching hacking tools to various components of the ATM.

Attacks against ATMs can also take a variety of forms. Attackers can deliver malware by compromising the banking network connected to the device, by compromising the device's connection to card processors or by gaining access to the ATM's internal computer. Much like traditional attacks, attackers or malware is often needed to escalate privileges on the victim device to gain deeper access into the system. This is where the use of malicious or vulnerable drivers comes into play. By taking advantage of the functionality insecure drivers, attacks or malware can gain new privileges, access information and ultimately steal money or customer data.

Attackers exploited security flaws in ATMs made by Diebold Nixdorf and NCR to modify the amount of currency being deposited to a payment card known as deposit forgery attacks. The vulnerability indicated that the problem is due to the fact that the affected machines do not encrypt, authenticate or verify the integrity of messages between Diebold's cash and check deposit module (CCDM) and NCR's bunch note accepter (BNA)] and the host computer.

1. NCR SelfServ ATM Attack

Overview

NCR SelfServ automated teller machines (ATMs) running APTRA XFS 04.02.01 and 05.01.00 are vulnerable to physical attacks on the communications bus between the host computer and the Bunch Note Accepter (BNA).

Description

NCR ATM SelfServ devices running APTRA XFS 04.02.01 and 05.01.00 contain vulnerabilities that can be exploited by an attacker with physical access to the internal components of the ATM specifically the BNA and the host computer.

- CVE-2020-10124: NCR SelfServ ATMs running APTRA XFS 05.01.00 do not encrypt, authenticate, or verify the integrity of messages between the BNA and the host computer. A similar vulnerability is identified as CVE-2020-9062 in VU#221785. CVE-2020-9062 involves the cash and check deposit module (CCDM) in ATMs from a different vendor. The CCDM is functionally similar to the BNA.

- CVE-2020-10125: NCR SelfServ ATMs running APTRA XFS 04.02.01 and 05.01.00 implement 512-bit RSA certificates to validate BNA software updates. Keys of this strength can be broken by an attacker in a sufficiently short period of time thereby enabling the attacker to sign arbitrary files and CAB archives used to update BNA software as well as bypass application whitelisting, resulting in the ability to execute arbitrary code. (CWE-326)

- CVE-2020-10126: NCR SelfServ ATMs running APTRA XFS 05.01.00 do not properly validate software updates for the BNA. An attacker with physical access to internal ATM components can restart the host computer. During boot, the update process looks for CAB archives on removable media and executes a specific file without first validating the signature of the CAB archive. This allows an attacker to execute arbitrary code with SYSTEM privileges. (CWE-305)

Impact

An attacker with physical access to the internal components of the ATM, including the BNA, can execute arbitrary code. An attacker may also be able to commit deposit forgery, with or without executing arbitrary code.

A deposit forgery attack requires two separate transactions. The attacker must first deposit actual currency and manipulate the message from the BNA to the host computer to indicate a greater amount or value than was actually deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of currency. This second transaction may need to occur at an ATM operated by a different financial institution (i.e. a not-on-us or OFF-US transaction).

Recommendation

1. Apply an update: Update software to APTRA XFS 06.08. The update increases the strength of the RSA keys to limit the window of opportunity for an attacker to crack and misuse the keys (CVE-2020-10125). The update also provides protection against the bypass of the digital signature check (CVE-2020-10126). Software, hardware, firmware and configuration updates may be necessary, depending upon the current state of a specific vulnerable ATM.

2. Update software and hardware: APTRA XFS 05.01 stopped receiving support in 2015. Any customers still using unsupported software and hardware should upgrade at the earliest possible opportunity.

3. Update firmware: APTRA XFS Dispenser Security Update 01.00.00 contains the following firmware updates:

    1. USBCurrencyDispenser 04.01.01, firmware 0x0167 (for S1 dispensers)
    2. USBMediaDispenser 03.04.00, firmware 0x0118 (for S2 dispensers)

4. Update configuration: In addition to Dispenser Security Update 01.00.00, the Dispenser Protection Level and Dispenser Authentication Sequence parameters should be properly configured. The recommended configurations are:

    - Dispenser Protection Level: Level 3 (Physical Protection) for S1 and S2 dispensers
    - Dispenser Authentication Sequence: Sequence 2 or higher (for S1 dispensers), or Sequence 1 or higher (for S2 dispensers)

2. Diebold Nixdorf ATM Attack (VU#221785)

Overview

Diebold Nixdorf is the world's largest ATM maker. New attacks have been observed to use on ProCash 2100xe USB ATM terminals, with the attackers connecting to the device via USB ports. Diebold Nixdorf 2100xe USB automated teller machines (ATMs) are vulnerable to physical attacks on the communication channel between the cash and check deposit module (CCDM) and the host computer. An attacker with physical access to internal ATM components may be able to exploit this vulnerability to commit deposit forgery.

Description

Diebold Nixdorf ProCash 2100xe USB ATMs running Wincor Probase version 1.1.30 do not encrypt, authenticate or verify the integrity of messages between the CCDM and the host computer. An attacker with physical access to internal ATM components can intercept and modify messages, such as the amount and value of currency being deposited, and send modified messages to the host computer.

A similar vulnerability identified as CVE-2020-10124 is described in VU#815655. CVE-2020-10124 affects the bunch note acceptor (BNA) in ATMs supplied by a different vendor. The BNA is functionally similar to the CCDM.

Impact

By modifying deposit transaction messages, an attacker may be able to commit deposit forgery. Deposit forgery attacks happen when fraudsters can tamper with an ATM's software to modify the amount and value of currency being deposited on a payment card. Such an attack requires two separate transactions. The attacker must first deposit actual currency and modify messages from the CCDM to the host computer to indicate a greater amount or value than was actually deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of currency. This second transaction may need to occur at an ATM operated by a different financial institution (i.e., a not-on-us or OFF-US transaction).

Recommendation

1. Apply software updates to secure communications between the CCDM and the host computer.
2. Limit physical access to the ATM (including internal components), adjusting deposit transaction business logic, and implementing fraud monitoring.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organisation or individual that has access to ATM related malware share it with us through our email: info@serianu.com to allow us analyze and share IOC's.

Below are images showing tampering with the ATM machines to gain access: