Issued 11/23/18

85 Percent of ATMs Can Be Hacked in Under 15 Minutes via Network

The vast majority of Automated Teller Machines (ATMs) manufactured by NCR, Diebold Nixdorf, and GRGBanking and used by banks as cash dispensers have been proven to be easily hacked by potential attackers either remotely or locally, most times in under 15 minutes. According to Positive Technologies' analysis, ATMs are vulnerable to four categories of security issues ranging from insufficient peripheral and network security to system/device improper configurations and Application Control security bugs/faulty configuration. Roughly 85% of ATMs manufactured by NCR, Diebold Nixdorf, and GRGBanking are easily hackable in about 15 minutes by potential attackers when they have access to the ATM network. "If the attacker is an employee of the bank or Internet provider, this access can be obtained remotely," said Positive Technologies. "Otherwise, an attacker needs to be physically present to open the ATM, unplug the Ethernet cable, and connect a malicious device to the modem (or replace the modem with such a device)." After infiltrating the ATM, crooks can either make use of direct attacks targeting the ATM or the services running on it, or man-in-the-middle attacks that would allow them to intercept and modify data packets to spoof processing center responses and take control of the besieged device. Full details on the research team's findings are available on their "ATM logic attacks: scenarios, 2018" report.