NCR ATM Security Update

DATE: December 2019 **INCIDENT NO:** 2019-09 **REV:** #1

New Long Nose Overlay Skimmers

Summary

NCR is aware of a new type of overlay skimmer which fits the card bezel of the 20 and 30 series Skimming Protection Solution.

This style of skimmer is known as 'long nose skimmer.' The mounting point of the skimming read head of the long-nosed skimmer is designed to rest out of range of the SPS jamming and detection circuits, allowing the skimmer to operate successfully.

Long nose skimming is an additional attack type in the long list of skimming techniques (see NCR's Card Skimming Landscape Whitepaper for additional information)

Long nose skimmers have been found in Turkey and in Egypt on 6634 ATMs. NCR is also aware of black-market websites which describe these skimmers as being intended for markets in the Middle East and Canada. This website also markets the skimmer with a corresponding PIN capture camera which fits between the cash slots of the 6634.

There is no evidence that 6623, 6627, 6682 and 6687 models are affected. NCR's latest 80 series family of ATMs is also unaffected.

Guidance and Recommendations

As an immediate mitigation, there are fascia inserts available from PinGuard, a third-party product provider, that block the space for this pin capture camera.

NCR is also working on alternative mitigations. An SPS adder is in development, which is a mechanical addition to the SPS bezel. This adder removes the linear card motion required by the skimmer and has features that work in conjunction with the SPS to prevent its removal. NCR expects first customer samples of this device to be available in February 2020.

NCR is also investigating the possibility of putting additional sensing into the SPS bezel to detect long nose skimmers. The feasibility of this proposal is unknown at this time, and NCR will release additional communication as soon as enough information is available for a decision to be made.

Long nose skimmers are another example of criminal technological progress in the field of card skimming. There is no reason to believe that criminals will stop developing new skimming techniques for as long as card skimming remains viable to capture authentication credentials at the ATM. The root cause of skimming vulnerabilities is the presence of the magnetic strip on payment cards, and card issuers should begin to roadmap the discontinuation of this out of date technology.

EMV is an effective technology for authentication at ATMs. EMV cards cannot be cloned because each card contains a unique key that is used to create a unique cryptogram for each transaction. The full benefit of EMV technology can be realized in today's environment if coupled with chip only card readers, geo-blocking, or contactless EMV. Please see the accompanying white paper for more details on these strategies.

Contacts

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

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