NCR ATM SECURITY UPDATE

DATE: November 27, 2017 **INCIDENT NO:** 2017-10 **REV:** #1

New Intel Vulnerabilities

Summary

In response to issues identified by external researchers, Intel has released a security advisory INTEL-SA-00086 that lists new vulnerabilities in Management Engine as well as bugs in the remote server management tool Server Platform Services, and Intel's hardware authentication tool Trusted Execution Engine.

General Guidance and Recommendations:

This Intel vulnerability is limited to Skylake/Kabylake chip. This chip in **not** currently in use with most NCR ATMs. This chip is in some use for customers who have a custom configuration. Customers who may be impacted by this have been notified by NCR and have taken preventive measures to protect from the vulnerability.

NCR ATM deployers are again reminded that Logical Attacks like these malware attacks can be mitigated by following the guidelines provided in the **NCR Logical Attack Protection Whitepaper.**

Customers who would like to get additional guidance as to their current state of security deployment and how it aligns with NCRs best practices are encouraged to request a complimentary **ATM Security Assessment**.

NCR ATM SECURITY UPDATE

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

Contacts

ATM Crime Reporting : global.security@ncr.com

Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com

Further information on this alert please contact Owen Wild

Please refer any media inquiries or questions to Aaron Gould

NCR ATM SECURITY UPDATE