# NCR ATM SECURITY UPDATE

**DATE:** June 24, 2019 **INCIDENT NO:** 2019-03 **REV:** #1

# New Intel Chip Security Vulnerabilities – Microarchitectural Data Sampling (MDS)

## Summary

NCR is aware of coverage reporting that security researchers have found a new class of vulnerability in Intel chips which, if exploited, can be used to steal sensitive information directly from the processor. The new vulnerabilities are a new subclass of speculative execution side channel vulnerability known as "Microarchitectural Data Sampling" (MDS) vulnerabilities. MDS are side-channel attacks targeting Intel chips, allowing hackers to effectively exploit design flaws in the processor architectures to extract sensitive data using malware.

The vulnerabilities are made up of four CVEs (CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2018-11091), which form the three named vulnerabilities **"ZombieLoad", "RIDL",** and **"FALLOUT"**.

Almost every computer with an Intel chip dating back to 2011 is affected by the vulnerabilities. AMD and ARM chips are not said to be vulnerable, like earlier side-channel attacks. The list of processors affected, and for which there will be updates, is extensive and can be found at the following location https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

NCR ATMs use chips that have been identified in these CVEs and Microcode updates will be made available for **Pocono, Riverside, Estoril, Falcon** and **Skylake** cores (these representing the majority of deployed NCR ATMs). Updates beyond these cores will be evaluated if, and as, needed.

Microsoft released new patches in May 2019 that specifically mitigate this vulnerability: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013

# NCR ATM SECURITY UPDATE

These patches include guidance that amounts to ***"apply any patches and microcode updates made available".***

## General Guidance and Recommendations:

Current analysis indicates that if customers follow NCR's best practice guidelines and deploy the security updates provided, then their ATMs will be protected against this set of MDS vulnerabilities. In order to mitigate these vulnerabilities, customers should perform all three of the following items:

1. Deploy the patches made available by Microsoft (14th May 2019) as soon as possible.
2. Deploy BIOS updates when they are available.

   The updated BIOS should be deployed, once available, in addition to the Microsoft Security Updates. NCR customers should contact their NCR Account Managers or Professional Services contact to get additional information on the availability of these BIOS updates.

   If a customer does not have our Secure Remote BIOS Update solution, then these BIOS updates may require on site visits to the ATMs. Customers should be urged to consider deploying NCR Secure Remote BIOS Update to further reduce the ongoing costs and operational impact of manual updates.

   If a customer does have our Secure Remote BIOS Update solution, this will enable remote distribution and deployment of the new BIOS. We are making updates to the NCR Secure Remote BIOS Update solution to enable remote delivery of the new BIOS to the ATMs, and availability dates will be advised ASAP.
3. Disable Hyperthreading on the affected machines. If the patches referred to in 1 and 2 above cannot be applied immediately disabling hyperthreading on its own IS a mitigate that should be put in place as an initial measure.
   **Note:** Disabling hyperthreading will have a performance impact.

# NCR ATM SECURITY UPDATE

As with previous speculative execution vulnerabilities, the issue is only *fully* mitigated after all 3 items are applied. Until all items are applied this attack is *partially* mitigated by the OS level patches supplied by Microsoft, *partially* mitigated by deploying the BIOS microcode patch supplied by Intel, and by turning off hyperthreading. All three of these steps **MUST** be applied in order to entirely prevent exploitation.

As attacks require malicious software to become present and execute on an ATM in order to exploit the vulnerability, the key to preventing exploitation is to prevent such malware being installed. If it is not possible to perform all the above items immediately, following NCR's best-practice guidelines detailed within the NCR Logical Security - Requirements to Protect Against Logical Attacks document. It will also provide protection against the exploitation of these vulnerabilities while patches become available. During this period, apply any patches as soon as possible after they become available.

Customers with Managed Services provided by NCR should reach out to their SWD (Software Distribution) Account representative to have a deployment schedule created.

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: NCRSelf-Service.Security@ncr.com
Please refer any media inquiries or questions to Warner D. May