NCR ATM SECURITY UPDATE

DATE: January 5, 2018 **INCIDENT NO:** 2018-01 **REV:** #1

New Chip Security Vulnerabilities

Summary

NCR is aware of the reports of new security vulnerabilities within computer chips produced by Intel, Advanced Micro Devices and ARM holdings. These vulnerabilities are identified as:

CVE-2017-5753
CVE-2017-5715
CVE-2017-5754

NCR ATMs use chips that have been identified in these reports.

Microsoft released security updates on January 3rd 2018 to mitigate against these vulnerabilities. Guidance from Microsoft is available at:

https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

NCR is currently lab testing the security update provided by Microsoft. Once testing is complete, NCR will send out a notification via our Microsoft Hot fix mailing list to indicate that testing was successful.

Current analysis indicates that if customers follow NCR's best practice guidelines and deploys the security updates provided by Microsoft on 3rd January 2018, their ATMs will be protected against this vulnerability.

NCR ATM SECURITY UPDATE

General Guidance and Recommendations:

Customers should:

1. Deploy the January 3rd 2018 patches made available by Microsoft as soon as possible.

2. Follow NCR's best-practice guidelines detailed within the *NCR Logical Security: Security Requirements to Help Protect Against Logical Attacks*.

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

NCR customers that subscribe to the NCR Software Distribution managed service are automatically protected from this attack.

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