



Critical Security Vulnerabilities—Meltdown & Spectre Update

Informa 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 3, 2018 to migrate against these vulnerabilities. Microsoft has since suspended Windows security updates related to this issue on systems with older AMD CPUs, after a documentation mix-up led to the systems being unable to boot after patches were applied.

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

For all of our customer running Managed Services, our Remote Team will be deploying patches for Intel & Microsoft Windows 7 when certified by NCR. Any other security fixes in the interim we will be deploying through Managed Services.

This is another key benefit of running Managed Services as it protects our customers and they will receive these patches at NO CHARGE.



Reduce Risks from Outside Hackers!

- ✓ Monthly Windows security updates and service packs installed automatically
- ✓ Never forget to install an update
- ✓ Full quarterly reports satisfy ATM compliance for Auditors

Ask your Account Rep about how RemoteView can help to keep your ATM's secure from potential harmful vulnerabilities. Please call at (800) 643-7489.