FAQs on the Meltdown and Spectre Vulnerabilities

Checklist to help protect your bank

A major security flaw has surfaced in January that's thought to affect all Intel microprocessors since at least 2011, some ARM processors and AMD processors. The exploits, called Meltdown and Spectre, take advantage of the processors' hardware rather than a software flaw, so they circumvent security schemes built into major operating systems. News about Meltdown and Spectre have wreaked digital havoc while leaving many financial institutions and IT staff unsure what to do. These are complex vulnerabilities and the fixes that do exist have come in patchwork fashion, creating a lot of angst throughout the tech world.

Banks are always a high-profile target for cybercrime. To help you and your IT team gain clarity and proactive steps to offset some of the risks, 21 CFS has compiled a quick check list and FAQs to get your started.

What are Meltdown and Spectre? In simplest terms, they are two vulnerabilities that have been identified in the native architecture of ALL Intel and AMD PC Chips. Design flaws have left a tremendous portion of computer processors vulnerable to these two major exploits.

What is the danger? Spectre and Meltdown can allow an intruder access to secure data held in cached memory (usernames, passwords, financial data etc.). They both open up possibilities for dangerous attacks that exploit Meltdown to view data owned by other users and even other virtual servers hosted on the same hardware, which is potentially disastrous for cloud computing hosts. Beyond the potential specific attacks themselves lies the fact that the flaws are fundamental to the hardware platforms running beneath the software we use every day.

Who is vulnerable? Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Any PC or device with Intel or AMD chips, phones, tablets, PCs and servers are at risk. And depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

What can I do? Ensure proper network and system security and practice good messaging hygiene. Google, Microsoft and Apple are said to have released updates to their software to help mitigate Meltdown and Spectre.

What is my responsibility as an Executive? Contact your IT Security provider whether internal or external and ask for a statement of their plan to mitigate. This plan should include items such as:

a. Firewall Firmware up to date and rules validated and reviewed

b. All perimeter network security hardware evaluated for currency of firmware and software

c. Ensure malware/virus protection systems are up to date

d. Provide guidance on good messaging hygiene (no opening email from unknown senders, etc.)

e. Thoroughly test and evaluate all Firmware BIOS and OS patches and updates BEFORE approving for install into production

By now, one thing we know for sure is that dealing with vulnerabilities is a moving target. Every day seems to bring new, relevant information that must be factored into ongoing mitigation efforts. If you or your bank's IT staff have any questions regarding the Spectre and Meltdown vulnerabilities, please give us a call.

21CFS
INNOVATIVE BANKING

10711 Burnet Road, Suite 306 • Austin, TX 78758 • Direct: 512.490.2505 • Toll free: 866.398.2178 • 21cfs.com • sales@21cfs.com