Spectre and Meltdown

Cyber security's most wanted

By Peter Morin, Senior Manager, and Adil Palsetia, Partner, KPMG in Canada

Spectre and Meltdown are fast becoming two of the most notorious names in cyber security history. And while it may be some time before these hardware vulnerabilities are fully addressed, there are actions that organizations can take now to mitigate the potential fallout.

But first, some background. Spectre and Meltdown are hardware vulnerabilities related to a flaw that exists within virtually all computing processors made since 1995 regardless of the operating system used or whether it is a laptop, desktop or server. These vulnerabilities are uniquely broad in scope affecting nearly every computer and device with a modern processor: Microsoft Windows, Google Android, Google ChromeOS, Apple macOS, on Intel, AMD and ARM processors.

To understand this flaw is to understand the threat Spectre and Meltdown pose. Essentially, the moment data is entered into a computer, it passes through the CPU and is stored in the computer's cache memory. When sensitive information such as passwords or encryption codes are entered into an online field, that raw data exists in an unsecured state on the user's computer before it is transmitted securely.

In theory, modern processors and operating systems are designed to isolate that vulnerable memory from every program and operating system. However, the use of a modern processing technique called 'speculative execution' – which performs computing tasks before they are needed – is now known to create a change in the processor state that can 'tip off' malicious programs as to where sensitive data is being kept within a system's memory functions.

Spectre and Meltdown make use of this design flaw. Meltdown 'melts' the security barriers that are enforced at the hardware level while Spectre does the same with barriers between user applications and the operating system.

Sound the alarm

The potential risks of Spectre and Meltdown are clear. By making sensitive data easier to find, this flaw makes sensitive data easier to steal. Computers connected to a virtual network can also be used as a bridge to larger targets. For example, if an otherwise secure and legitimate online shopping platform shares a cloud computing network with a less-than-secure (or outright malicious) website, that website could be used to steal data from the verified platform.

These vulnerabilities have been suspected for some time. Moreover, the cyber-attack methodologies that can be used to exploit them are well known in the hacker communities. What makes Spectre and Meltdown of particular concern are several factors:

Widespread impact: Many are calling Spectre and Meltdown the most widespread vulnerabilities in computing history – and for good reason. They impact every processor made in recent history and a number of chips already in production. This flaw is in virtually every computing device and has the potential to impact every personal computer user on the planet.

No easy fix (yet): Spectre is harder to exploit but the potential for serious damage is real. Patches and updates have already been issued to 'plug the leak', but the ultimate solution will require a complete replacement of systems and a fundamental change in the way future processors are made. Meltdown is easier to exploit, but can be fixed with a patch at the sacrifice of processing speeds. Neither of these current fixes is ideal and permanent solutions could be a long way away from hitting the market.

Cure at a cost: Eliminating the risks of Spectre will involve physically replacing systems, while patching vulnerabilities associated with Meltdown can cause processing speeds to slow down by upwards of 30 percent. The resulting impact on company functions will vary based on workload and system use, but these 'fixes' will likely translate directly into monetary losses.

The good news is that organizations with a strong vulnerability management program (with solid asset management and patch management capabilities) have a head start in reacting to these vulnerabilities. Those which do not, however, will find it difficult and overwhelming to patch existing systems without a streamlined patching strategy already in place.

A partner in cyber defense

Whether prepared for an attack or beginning to panic, there's much an organization can do to mitigate potential cyber events caused by Spectre and Meltdown.

To start, organizations need to assess, strengthen, and implement vulnerability management programs. IT departments need to quickly embed security controls or optimize security operations functions, while additionally playing a hands-on role in developing critical defense tools such as patch deployment roadmaps/timelines or threat intelligence methodology.

It will be years before the true scope of Spectre and Meltdown is revealed. Unfortunately, organizations do not have the luxury of being able to wait and see if these vulnerabilities will be exploited. The time is now to mount a defense; and only with the right partners and strategies will the threats posed by Spectre and Meltdown be kept at bay.

Resources:

www. spectreattack.com

Technical details: CVE-2017-5715 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715 & CVE-2017-5753 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753

www.meltdownattack.com

Technical details: CVE-2017-5754 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754

Contact us

Francis Beaudoin
National Leader,
Technology Risk Consulting
KPMG in Canada
E: fbeaudoin@kpmg.ca

Yassir Bellout
Partner, Cyber Security
KPMG in Canada
E: ybellout@kpmg.ca

Jeff Thomas
Partner, Cyber Security
KPMG in Canada
E: jwthomas@kpmg.ca

Adil Palsetia
Partner, Cyber Security
KPMG in Canada
E: apalsetia@kpmg.ca

Peter Morin
Director, IT Advisory KPMG
in Canada
E: petermorin@kpmg.ca