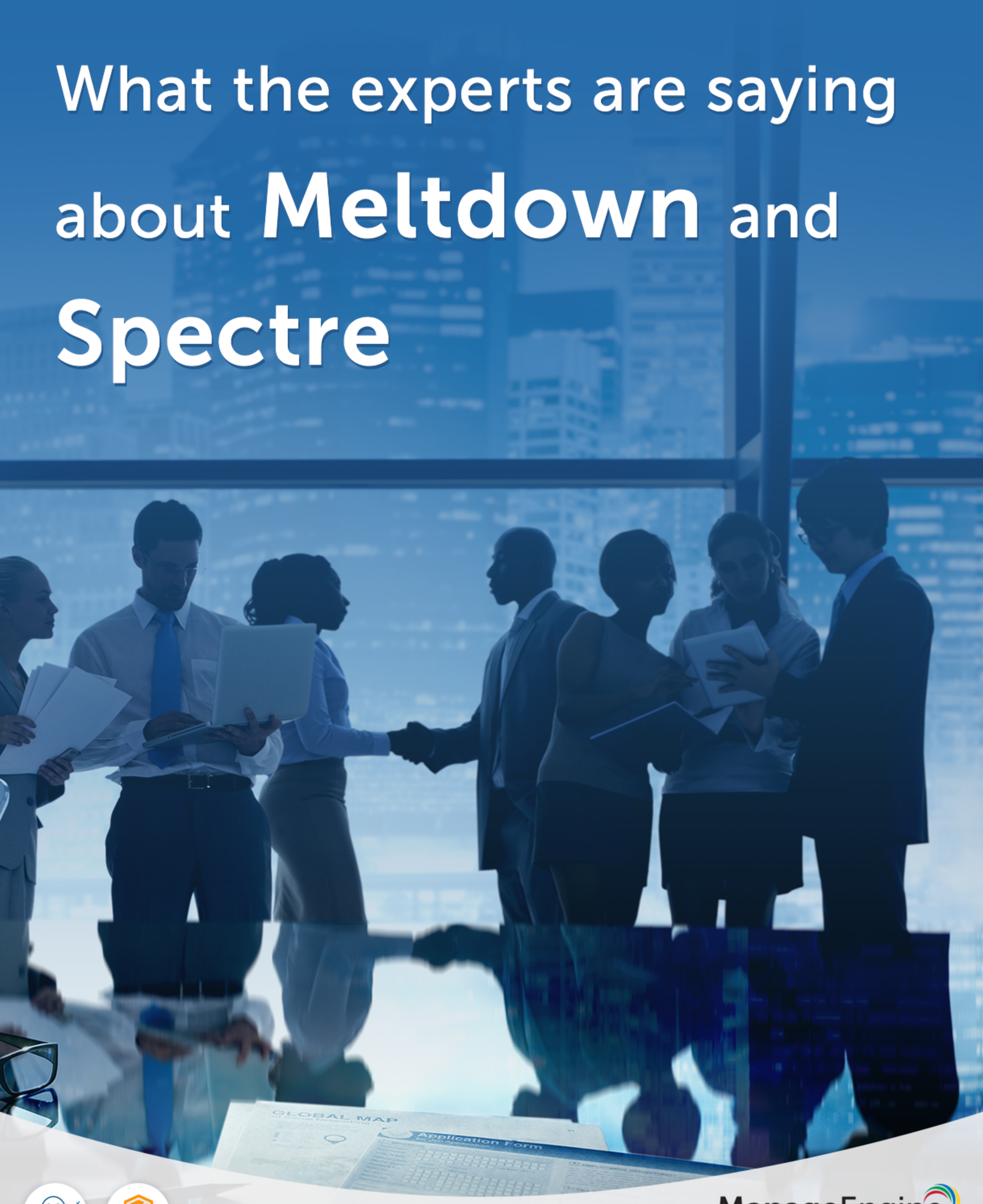
What the experts are saying about Meltdown and Spectre



ManageEngine
IT Management, Simplified

What the experts are saying about Meltdown and Spectre

The start of 2018 has been nothing short of exciting for the cybersecurity industry after Google Project Zero's infamous report on two existing CPU bugs. Spectre and Meltdown, two major processor flaws discovered in Intel, AMD, and ARM processors, allow attackers to access sensitive data that is handled by the CPU.

While there are number of articles, blogs, white papers, and e-books available on these processor bugs, ManageEngine is bringing you this vendor-neutral digest on leading IT security and cybersecurity researchers' thoughts and advice on Meltdown and Spectre. Hear what the experts have to say on how these flaws can impact businesses, and what IT professionals need to do to mitigate Meltdown and Spectre.

Harjit Dhaliwal (Microsoft MVP, senior systems administrator)

If you've been closely following the news, especially news related to technology, then you're probably already aware of the Meltdown and Spectre security vulnerabilities, which were disclosed at the beginning of this year. You can read more details about these flaws and how they work on Google’s Project Zero.

Basically, the flaws exploit~~s~~ what is technically a feature of modern processors to allow faster processing computation known as speculative execution, which is when a processor guesses your next operation based on previously cached iterations before it even happens. Typically, programs are not permitted to read or access data from other programs, however malicious attackers could take advantage and exploit the sensitive information stored in your memory, including passwords, banking information, and much more.

Security researchers have revealed that nearly every computer chip manufactured in the last 20 years contains this fundamental security flaw, which affects personal computers, servers, mobile devices, and cloud computing. This flaw can be found in processors designed by Intel, AMD, and ARM.

The following are advisories by the three key chip manufacturers:

- Intel : https://newsroom.intel.com/news/intel-responds-to-security-research-findings/
- AMD: http://www.amd.com/en/corporate/speculative-execution
- ARM: https://developer.arm.com/support/security-update

At the time of writing, there are no confirmed cases of hackers exploiting these security vulnerabilities, however you should never let your guard down and assume it's not going to happen. Everyone who uses a computer or any device with a processor should heed the advice and guidance provided by various computer and mobile device manufacturers, as well as software and operating system vendors, such as Microsoft, Apple, Red Hat, and VMware.

IT professionals and systems administrators have been working tirelessly to secure their systems and protect their environments. The process has been challenging and daunting due to the number of steps required, including operating system patches, updated antivirus solutions, firmware updates, and registry fixes. In terms of Windows-based systems, it's important to note that Microsoft requires that antivirus solutions are up-to-date and compatible before installing the January 2018 security updates to address Meltdown and Spectre. This requirement is to help prevent antivirus applications from making unsupported calls into the Windows kernel memory, which could cause system blue screens and, in some cases, unbootable devices. Microsoft provides a bulletin with plenty of details concerning this issue.

Customers will not receive the January 2018 security updates (or any subsequent security updates) and will not be protected from security vulnerabilities unless their antivirus software vendor sets the following registry key:

Key="HKEY_LOCAL_MACHINE"
Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat"

Value="cadca5fe-87d3-4b96-b7fb-a231484277cc" Type="REG_DWORD”
Data="0x00000000”

Hardware vendors such as Dell, HP, Lenovo, Acer, and others have been busy working to provide firmware updates as quickly as they can. Some firmware updates have been released while others have been recalled due to an issue which causes certain systems to reboot unexpectedly. It is strongly advised that you check with your hardware manufacturer for a valid, up-to-date firmware patch to apply to your systems. The resources listed below will help you with further information and guidance.

Microsoft: Protect your Windows devices against Spectre and Meltdown
Windows operating system security update for AMD-based devices
Apple : Apple security pdates
Google : Meltdown/Spectre vulnerability status for Chrome OS devices

Keep an eye out for news from the industry concerning this security threat, and secure your systems to help mitigate the risks.

Debra Baker (CISSP CCSP cybersecurity evangelist)

Spectre and Meltdown are major vulnerabilities in Intel, AMD, Qualcomm, and ARM processors. Because Spectre and Meltdown affect almost all processors, potentially all computers are susceptible to these flaws. CVE-2017-5753 and CVE-2017-5715 are collectively known as Spectre. The third vulnerability, CVE-2017-5754, is known as Meltdown. These vulnerabilities are all variants of the same attack and differ in the way that speculative execution is exploited.

Beyond the hype, what does it take to exploit these vulnerabilities? Spectre entails malware being installed on a device in order to exploit the vulnerability. What this means is that networking devices such as routers, switches, and servers would have to be compromised by a trusted administrator. Many network devices won’t run rogue unauthorized software, but even if they did, the administrator would either have to be tricked into installing the software, or deliberately install it.

All network devices and servers should be deployed in a physically secure data center, thus limiting who has access to your devices. In addition, strong password complexity rules should be set as well with no default passwords in use. If someone gets physical access to a device, they will soon have root access. Now, if the malware is installed on the device, then an unauthorized process can run and steal information from the memory space that it typically wouldn't be able to access.

The biggest threat vector is virtualized environments. In the event that one virtual machine in a cloud-hosted environment is infected, there's potential that the memory of the host OS could be read and leak information. The biggest threat is that Spectre is accessible from a browser using JavaScript. The end user would have to be tricked into downloading the malware onto their computer before the exploit can be executed.

Kim Crawley (Cybersecurity journalist)

The most overwhelming part about these vulnerabilities is that they've existed for so many years and we've been unaware of them.

eltdown has affected Intel x86 CPUs for twenty years, and Spectre is even more baffling. Some experts say that it can be partially mitigated with software patches while others claim the only option is to replace the hardware. These really are fundamental security flaws, much more fundamental than the vast majority of vulnerabilities I write about. They exist directly in how CPUs do their work. That's the most critical part of any computer.

Both bugs are connected to how CPUs engage in speculative execution. Companies like Intel, AMD, and Qualcomm have found that speculative execution is a useful feature for CPUs to have, so the feature isn't going away. The key to avoiding future vulnerabilities like Meltdown and Spectre is to get cybersecurity professionals more involved in the research and development of CPUs. Operating system vendors like Microsoft, Apple, and Google can only do so much as they work primarily in code, not in the R&D of the CPUs themselves.

Apple and Google also make hardware, but they buy x86 and ARM CPUs that are made by other companies.

So it's important for Microsoft, Apple, Google, Cisco, and Linux kernel developers to deploy any possible software patches for these vulnerabilities, but the ultimate responsibility is with the CPU vendors. If I was working in Intel R&D, I'd hire the people who discovered Meltdown and Spectre to work directly in my department.

Computer technology only gets more complicated as time goes on—it's inevitable. The Intel 486 Windows PC I used as a child is a lot more complicated than ENIAC, and my Sony Android smartphone is more complicated than that 486 PC from my childhood. As computer technology gets more complicated, cyber attack vectors multiply and cybersecurity itself gets more complex. I believe that Meltdown and Spectre are just a taste of what's to come in the next few decades.

So someone at Intel had better hire those Meltdown and Spectre researchers!

Shira Rubinoff (President at SecureMySocial, cybersecurity advisor)

It’s important to understand the difference between Meltdown and Spectre.

Meltdown, as its name suggests, breaks down the mechanism that keeps the applications from gaining access to random system memory. Once that happens, the applications can then access information in the system memory including passwords, pictures, emails, instant messages, business critical documents, and more. Spectre tricks applications into accessing random locations in their memory. Meltdown and Spectre work on personal computers, mobile devices, and cloud devices. They also utilize side channels to acquire the information from the obtained memory location.

Both Meltdown and Spectre highlight the need to ensure all systems and devices are upgraded with the latest software and patches. It's important to stay diligent on these updates so that our systems are not vulnerable to these types of attacks on a software and patch level. Many reports about Meltdown and Spectre highlight the importance of collaboration. These kinds of vulnerabilities were found by researchers at companies, security firms, and universities. Collaboration across the industry must become the norm to ensure latest security measures are being implemented across all sectors.

Why is it called Meltdown?

This vulnerability essentially melts security boundaries which are normally enforced by the hardware.

Why is it called Spectre?

The name is based on the root cause: speculative execution. As it is not easy to fix, it will haunt us for quite some time.

Summary

Based on this in-depth look at Meltdown and Spectre, it's clear that the experts agree on one thing: deploying the correct patches for your operating systems, BIOS, and firmware is one of the best ways to keep your sensitive data safe. There are already reports that as many as 139 different samples of malware exploiting Meltdown and Spectre are already in existence, so now is the time to patch your systems.

Please refer to this collection of frequently asked questions if you have any further questions regarding Meltdown and Spectre.