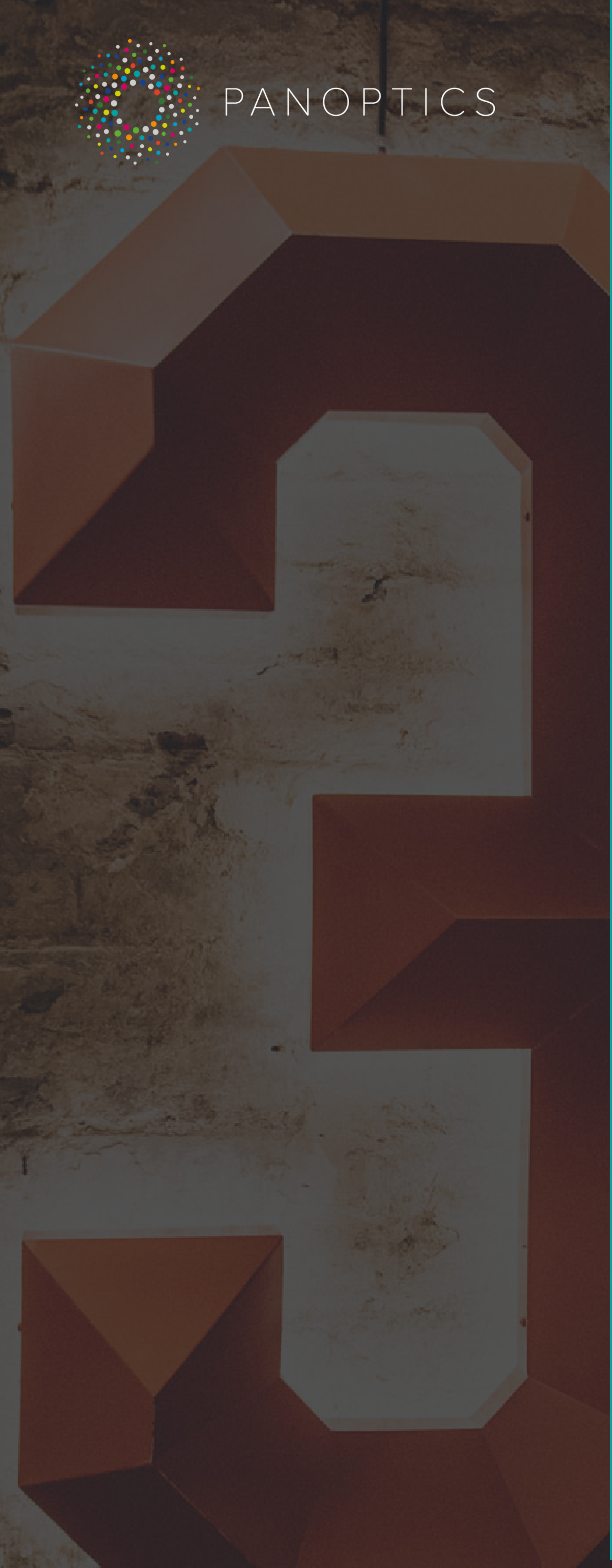
Call: 0203 137 6351

Email: hello@panoptics.com



Meltdown and Spectre: How to protect your environments

A practical guide to IT's latest security threat

In today’s all-connected world, the battle to protect data is as challenging as it has ever been. When everything from your PC to your kettle could be connected to the outside world, securing these devices and more importantly the business-critical and sensitive data they can give access to is a serious business.

Teams of security researchers all over the world work constantly to analyse existing vulnerabilities in an attempt to discover new threats, before they can be exploited and turned into a new form of Cyber Attack.

Recently, two new major threats were discovered that could potentially put all modern day computers and electronic devices at risk as the threat landscape continues to evolve.

So what are these threats, and how can we protect our valuable data against them?

What are Meltdown and Spectre?

Officially defined as CVE-2017-5753 and CVE-2017-5715 in the National Institute of Standards and Technology (NIST) National Vulnerability Database, the threat collectively known as Spectre describes the potential for a malicious actor to direct a specific targeted attack to a vulnerable system, with the intent to gain access to unauthorized data.

Spectre exploits a feature of the vast majority of modern processors that will attempt to ‘guess’ the result of a branch in computer code, and speculatively execute the resulting code segment. This functionality can be used to the attacker’s advantage to execute code that would not normally be permitted, and whilst the processor will in most cases ‘roll back’ the code the attacker could have already gained access.

The Spectre vulnerability exists at the microchip level, and as such most modern computers, servers and even smartphones and tablet devices are potentially at risk.

Despite this, to exploit Spectre and compromise a system would require specialist knowledge. An attack would need to be written and deployed to a specific target system, and in order to do so the attacker would need to be able to bypass existing physical and logical security measures already in place to protect these systems.

To fix the vulnerability, all affected systems will need to be updated with the vendor specific patches released in response to the disclosure of Spectre- in many cases, these fixes may have already been applied as part of a standard patching policy.

Along with Spectre vulnerabilities, researchers also discovered a related vulnerability known as Meltdown. Whereas Spectre affected nearly all modern processors, Meltdown only affects processors manufactured by Intel- this is however still a large proportion of processors used today in Computer and Server systems.

Officially defined as CVE-2017-5754 in the NIST Vulnerability Database, Meltdown could allow a malicious actor to gain unauthorised access to system memory and the data it holds by introducing ‘errors’ in code known as a trap. How the processor responds to these traps could allow an attacker to access areas of system memory normally inaccessible to user-level access, leading to the unauthorised extraction of data via a cache- which is the same method of data egress exploitable by Spectre and thus linking the two threats.

As with Spectre, Meltdown can be negated by applying vendor-specific patches to all affected systems in order to fix the vulnerability.

How to protect your environments

The good news is that the Spectre and Meltdown vulnerabilities were disclosed to vendors prior to them entering the public domain, and so in almost all cases patches are available to fix them.

The bad news is that there could be a fair amount of work to do in order to fully protect your environment, and your data.

Got a smartphone? Install the latest update and you’re covered. Running Linux? Make sure you update to the latest kernel version.

For Windows systems a little extra diligence is required. Initially there were issues reported with the patch leading to a ‘blue screen of death’ on some systems. This was traced to an issue with certain Anti-Virus software vendors and products, so in order to prevent these stop errors, AV vendor are forced to prove their software is ‘compatible’ with the patch by creating a registry key.

The Windows patch from Microsoft will only install if this registry key is present in your system. More importantly, automated patching solutions such as SCCM or WSUS will mark the patch as ‘not applicable’ for systems without the registry key, making it difficult to see where the patch has not been applied and could potentially prevent future updates from installing as well.

Before applying the patch then, check your AV vendor is compatible, and make sure your AV product is functioning and up to date.

Furthermore, for Virtual environments you will need to patch your virtual hosts not only to protect the host themselves from the vulnerabilities, but it’s also necessary for the Operating System patches installed in your Guest Virtual Machines to be fully effective.

If you need help in protecting your systems from Meltdown, Spectre or any other threat, please get in touch.

We're always available to discuss any IT Project and would welcome the opportunity to talk it through. Get in touch now and we're confident we will find the perfect solution for your business.

Get in touch today.

0203 137 6351
www.panoptics.com

PANOPTICS