



(<https://web.archive.org/web/20180226191857/https://www.nttsecurity.com/>)

Visit our Business blog

(<https://web.archive.org/web/20180226191857/http://insight.nttsecurity.com/>)



Meltdown and Spectre: one week later

12 Jan 2018

NTT Security



Guest post from Danika Blessman, Senior Threat Intelligence Analyst at NTT Security.

On January 3, 2018, Google's Project Zero released details about undisclosed vulnerabilities, Spectre and Meltdown, in multiple manufacturers' CPU chips. Tied together, these vulnerabilities essentially boil down to one thing: a weakness in the implementation of [speculative execution](#).

This leaves CPU hardware implementations vulnerable to side-channel attacks, allowing an attacker to read privileged memory. The nature of these vulnerabilities and their fixes introduces the possibility of reduced performance on patched systems. The performance impact depends on the hardware and the applications in place.

The Meltdown vulnerability affects Intel processors specifically, and works by breaking the barrier between user applications and the operating system itself, allowing an attacker to access the memory and information stored there.

Segregating and protecting memory spaces can help prevent this “break”, and also helps to prevent attackers from viewing or modifying this information. Meltdown makes this fundamental process unreliable.

Spectre affects Intel, AMD, and ARM processors, extending its reach to include mobile phones and embedded device. Spectre, however, works differently from Meltdown. Spectre essentially tricks applications into disclosing information which would normally be inaccessible within the protected memory area. This vulnerability is challenging to exploit as it is based on an established practice in multiple chip architectures.

These vulnerabilities enable attackers to execute code with user privileges and can have a wide range of impacts, such as reading otherwise protected kernel memory and bypassing kernel address space layout randomization (KASLR).

Attackers can also take advantage of speculative execution to read system memory which should have been inaccessible. For example, an unauthorized party may read sensitive information in the system’s memory such as passwords, encryption keys or sensitive information open in applications. Testing also showed that an attack running on one virtual machine was able to access the physical memory of the host machine and, through that, gain read-access to the memory of a different virtual machine on the same host. If you are operating in a cloud environment, this really is a big deal. If you are separating multiple customers in their own VMs, these attacks potentially allow the attacker to access memory across VMs. What that really means is that clients may be able to read data from other clients.

Variants of this issue are known to affect many modern processors, including certain processors by Intel, AMD and ARM. For a few Intel and AMD CPU models, there are exploits which work against real software. These issues have been reported to Intel, AMD and ARM.

So far, there are three known variants of the issue:

- Variant 1: bounds check bypass (CVE-2017-5753)
- Variant 2: branch target injection (CVE-2017-5715)
- Variant 3: rogue data cache load (CVE-2017-5754)

NTT Security is aware that Windows updates for AMD processors have resulted in systems not booting after updating and/or patching. Microsoft has suspended releases for AMD PCs and is waiting on an updated mitigation strategy from AMD.

Some, including the US Computer Emergency Response Team (US-CERT), suggest the only real fix for these issues is for the affected chips to be replaced, however this may be highly impractical for most users and organizations. Patching is currently the most effective way of mitigating these vulnerabilities.

But these fixes are not without catches.

Of significance is that some organizations are facing a remediation roadblock which will not allow current patches to be installed immediately – if at all – without causing undue risk of operational failure on their networks. This is a situation where it is essential for the organization to evaluate the vulnerability and the potential risk to the affected systems. If a patch cannot be installed relatively quickly, or is determined to be incompatible with existing applications or technology, the operational risk must be addressed via other means.

NTT Security recommends that an organization in the above scenario employs defensive practices such as network segmentation and access controls to reduce risk to the affected environment, if possible. NTT Security also recommends that continuous monitoring, detection and response be employed or increased for the affected systems and network environment.

Another potential roadblock that users may encounter, according to a Microsoft [statement](#) is that a small number of third party anti-virus vendors are not compatible with the Windows updates. Therefore, some users may not receive these updates.

Also of significance, since these vulnerabilities do not affect a specific operating system, is that solutions that monitor at that level will likely be incapable of detecting these types of attack.

These are considerable vulnerabilities, and based on the visibility Meltdown and Spectre has received, we expect researchers will greatly expand efforts to identify additional related vulnerabilities. This may mean the industry is faced with a continuing cycle of critical vulnerabilities, exploits and patches in the future.

Lastly, the performance impacts of the Microsoft patches are still being determined, but some sources have identified them as “significant”. If you are in a high demand environment, or nearing CPU capacity, applying these patches may necessitate the implementation of additional systems to meet your performance needs. The catch is that you will probably not know this until you measure performance after applying the patches in your own environment.

NTT Security released an Emerging Threat Advisory (ETA), along with two updates, to clients, outlining these vulnerabilities, potential impacts to systems, signatures and recommended actions.

In addition, NTT Security has provided detection signatures from vendors addressing the Spectre and Meltdown vulnerabilities.

NTT Security continues to monitor for additional signatures and additional detection technologies and will update its clients as appropriate.

To date, statements, advisories and/or mitigation efforts have been issued by a majority of affected vendors.

While it appears that Spectre and Meltdown are exceedingly difficult to defend against and mitigate, especially since traditional anti-virus may not detect an attack, effective patches are available for both. And many security researchers have concluded both Spectre and Meltdown are quite difficult to exploit in practice. This may suggest that both vulnerabilities may have limited real-world use, however, a sophisticated or well-funded attacker may be able to develop more efficient techniques.

To date, there have been no reported exploits in the wild, but a proof of concept code is publicly available.