Meltdown and Spectre

How to mitigate these processor flaws?

A whitepaper by ManageEngine

ManageEngine
Desktop Central

In the early days of 2018, Google Project Zero's discovery of two crucial flaws in several processor chips stole the limelight. As word of these vulnerabilities spread before an official announcement was made, efforts were in full swing to take on Meltdown and Spectre, two of the most serious flaws in the history of computer hardware vulnerabilities.

If exploited, Meltdown and Spectre could have devastating effects on almost any computer's confidential data by giving hackers a way to seize essential data without users' knowledge. Even as the exploitation happened at hardware level, the initial round of software patches helped reduce the impact of exploitation. While there are no cases of attackers exploiting these vulnerabilities yet, these flaws could lead to serious trouble if unattended to.

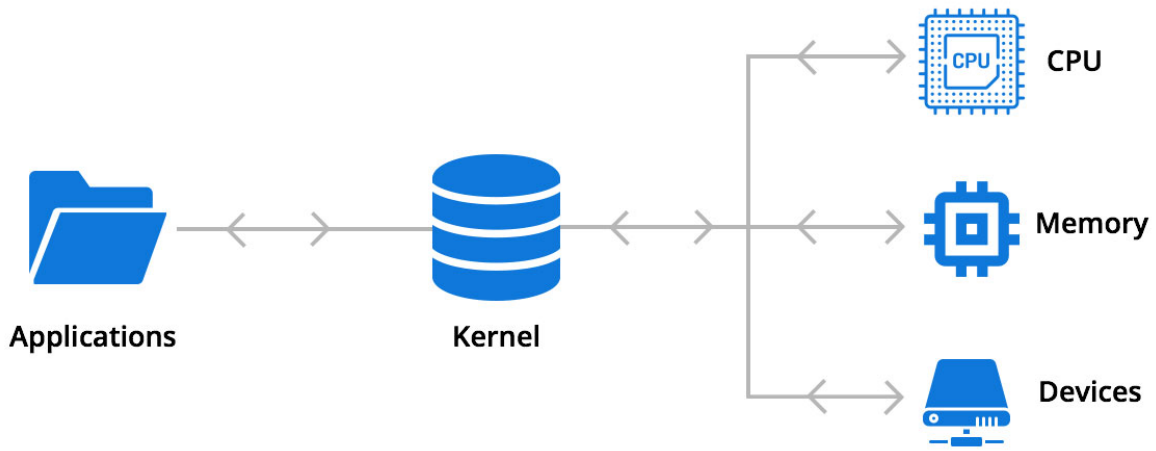
In this white paper, we'll discuss what Meltdown and Spectre are, how they could impact your machines, how tech companies have responded over the year, and how you can mitigate these vulnerabilities.

Meltdown and Spectre: An overview

Meltdown and Spectre aren't two different flaws per se, but rather variations of a single vulnerability that affects nearly all processor chips manufactured in the last two decades, including those made in the pre-internet era.

When it comes to Meltdown and Spectre, it helps to understand how computers work at a basic level. First things first: programs and applications work independently from each other. The OS kernel acts as an interface between applications and the computer's memory, CPU, and devices (as shown below). The kernel, which is the heart of the OS, runs in a privileged mode; this prevents processes from interacting with each other and protects access to device drivers and other hardware devices.

Meltdown got its name because it "**melts**" the **fundamental isolation between the OS kernel and applications**. Thus, programs can access the device's memory when they shouldn't be able to, rendering the sensitive data of the OS and other programs insecure. Spectre, on the other hand, is a **rupture in the isolation between applications**.



Speculative execution and caching

Meltdown and Spectre are largely the result of how processor chips are designed. Today, most processors are designed to offer better specifications in terms of clock speed; one way processors speed up processes is by performing speculative execution. Speculative execution helps processors complete tasks faster by predicting which branch will be taken and executed. If the prediction is right, the branch is persisted with; otherwise, the job is discarded and the correct branch is revisited.

Caching, like speculative execution, is another feature that helps processors run faster. At a basic level, caching is the process of hastening a CPU's access of memory. A CPU usually

takes more time fetching data from the main memory/RAM; for faster performance, the CPU can instead access the nearby cache memory. This memory space can be used for temporary storage of processed data, especially the computations resulting from speculative execution.

Consider this example: You go to a restaurant every day at a particular time and order the same sandwich for breakfast. The chef knows this and starts preparing the same sandwich every day and has it ready for you before you even arrive. By doing so, he minimizes the processing time required for making the food. However, if one day you choose to have a salad instead of a sandwich, he will have to discard the already prepared sandwich. Here, the sandwich is analogous to the processed data, which can be picked up by someone else and acted upon.

How do processors differ from the example above? Data processed via speculative execution can't just be "picked up" by another program or application. As mentioned earlier, the OS kernel prevents one program or application from reading another program or application's data.

Although the processor begins working with data even before the branching execution grants reading privilege, data is still protected throughout speculative execution. The processor only reads processed data after the right branch is executed. The trouble comes when the executed data is kept in the cache for quick retrieval by the processor.

By leveraging Meltdown and Spectre, attackers can exploit speculative execution and extract executed data stored in the CPU cache. While hackers can use Meltdown to access kernel memory, Spectre lets them trick an otherwise normally functioning program into leaking protected data. Both of these side-channel attacks let processes access information that they shouldn't be able to, so hackers can then siphon off that data.

Initially only 4 variants were discovered, but researchers went on to name a few more after the component targeted.

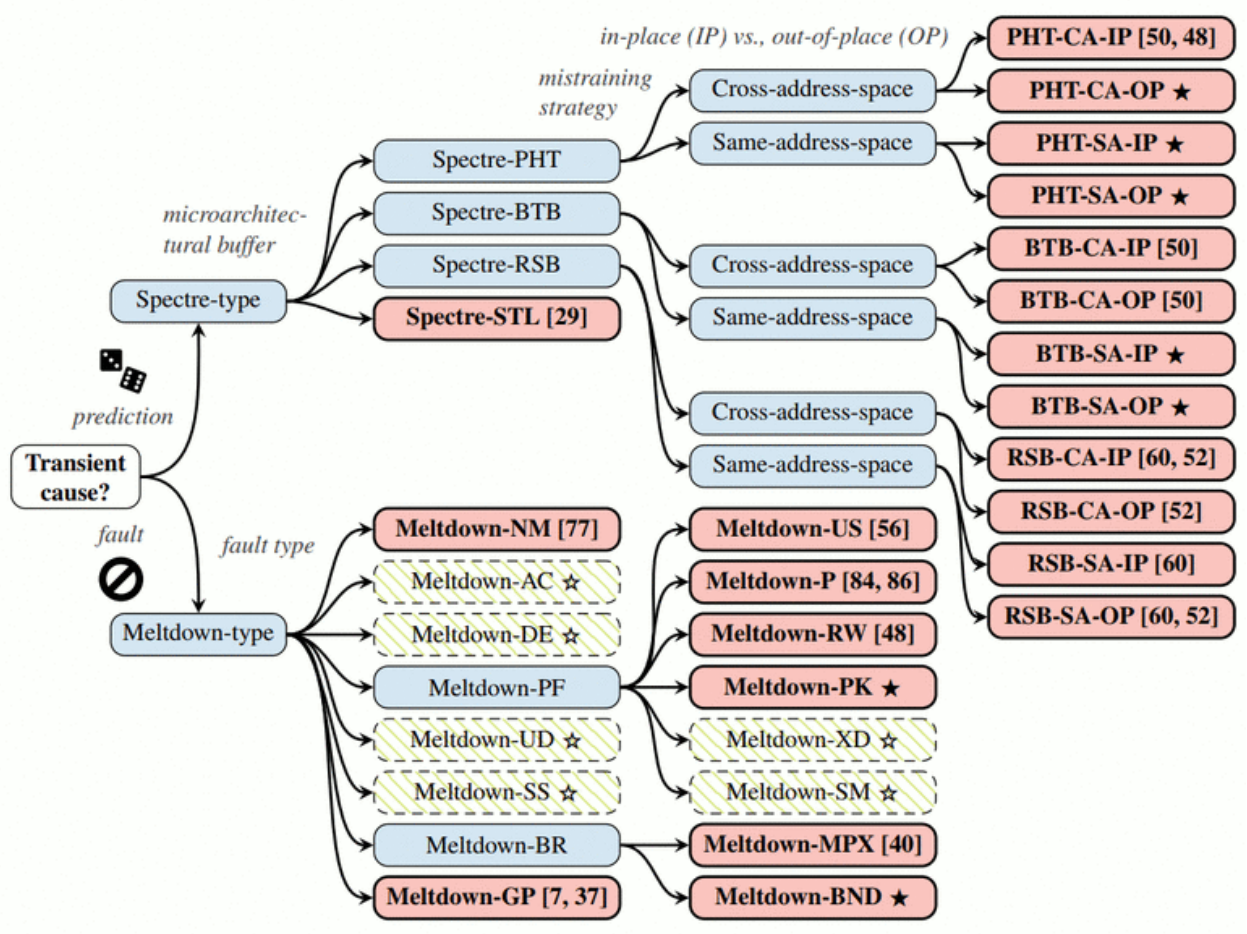


Image: Canella et al

The potential impact of Meltdown and Spectre

So far, Meltdown and Spectre have primarily affected processor chip companies, OS developers who released remedial patches, and cloud service providers . Both Meltdown and Spectre have the potential to lead to serious data leaks, including the disclosure of sensitive information like financial records, credit card numbers, email addresses, customer databases, cryptographic keys, and passwords.

Meltdown has widely affected computers using Intel, ARM chips. Unlike Meltdown, Spectre applies to all three major processor chips in the market: Intel, AMD, and ARM. Although Intel has recognized that their processors are vulnerable to these flaws, they have reassured consumers that, "These exploits have no potential to corrupt, modify or delete the data." AMD claims to have dodged the Meltdown attack due to basic differences at the

design level.

While some mobile devices don't use processors that support speculative execution (meaning that they don't appear to be affected by Meltdown and Spectre), many mobile devices—including iPads, iPhones, and non-Google Android devices—are vulnerable. New devices that use Qualcomm's latest processor, Snapdragon 845, are potentially at risk as well.

Remember how Meltdown allows unprivileged processes to read data in the memory? Well, that means that if you're running a server providing web services to hundreds of computers, then you are in a dangerous situation. Meltdown could be exploited to access data held in other virtual servers hosted on the same hardware, which is potentially disastrous for cloud computing hosts. If one customer runs malicious code, they can potentially read sensitive data from other customers or from your own servers. From the consumer side of things, hackers can also use malicious Java scripts that leverage Meltdown to steal passwords stored in browsers.

Tech giants' responses

- To take on Spectre, Intel released several microcodes to alter the behavior of branch prediction. The initial updates were disabled by Microsoft as they caused instability and sudden reboots. Later, more stable microcodes were released throughout 2018, even as new variants were discovered. These capabilities reportedly prevented branch predictor (hardware) from influencing the branching guess, raising a barricade before branch prediction happens.
  Intel also recently announced a new faster processor Sunny Cove Architecture that comes patched against Meltdown and Specre vulnerabilities.
- ARM said in a press release that it has been "working together with Intel and AMD to address a side-channel analysis method which exploits speculative execution techniques used in certain high-end processors. This is not an architectural flaw; this method only works if a certain type of malicious code is already running on a device and could at worst result in small pieces of data being accessed from privileged memory. ARM takes all security threats seriously and we encourage individual users

to ensure their software is up-to-date and always follow good security practices." ARM recommends that the software mitigations described in their Cache Speculation Side-channels whitepaper be deployed where protection against malicious applications is required.

- Microsoft released patches for different versions of Windows, and for browsers Internet Explorer and Edge. January patches caused crashes for various AMD machines(blue screen errors) Microsoft has included Retpoline patch - Google's mitigation for Spectre in its Windows 10 update. Here is a Windows utility Specucheck for checking the state of the software mitigations and hardware against Meltdown and Spectre variants.
- Apple's response against speculative execution vulnerabilities in ARM-based and Intel CPUs: Apple released mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 to help defend against Meltdown. Security updates for macOS Sierra and OS X El Capitan also include mitigations for Meltdown. To help defend against Spectre, Apple has released mitigations in iOS 11.2.2, the macOS High Sierra 10.13.2 Supplemental Update, and Safari 11.0.2 for macOS Sierra and OS X El Capitan. Apple declared that Apple Watch is not affected by either Meltdown or Spectre.
- High impact browser patches (57.0.4) were released for Firefox
- Google Chromebooks received KPTI mitigations against Meltdown.. Google also claims to have come up with Chrome OS patches which have no or little impact on performance.

  Google Chrome implements a feature called 'Site isolation' to shield against Meltdown and Spectre. This means Chrome consumes more RAM than before, slowing down the computer.
- Linux vendorsFedora, Ubuntu, and Debian, are came up with patch fixes, but most of them affected the CPU performance . Red Hat and Suse also implemented Retpoline patches. Linux Kernel 4.20 came up with a mitigation called Single Thread Indirect Branch Predictors (STIBP), which resulted in a degradation of performance up to 50% in Intel processors.
- VMware came upw with a set of patches (VMS-2018-0002 and VMS-2018-0004) for its VMware workstations. They have also released a performance assessment of CPU utilization.

Similarly, tech giants like Amazon, Google, Android, Lenovo, IBM, Dell, HP Enterprise, Cisco, and Citrix have all responded with their own patch fixes. You can view all their security bulletins and advisories at the bottom of this page.

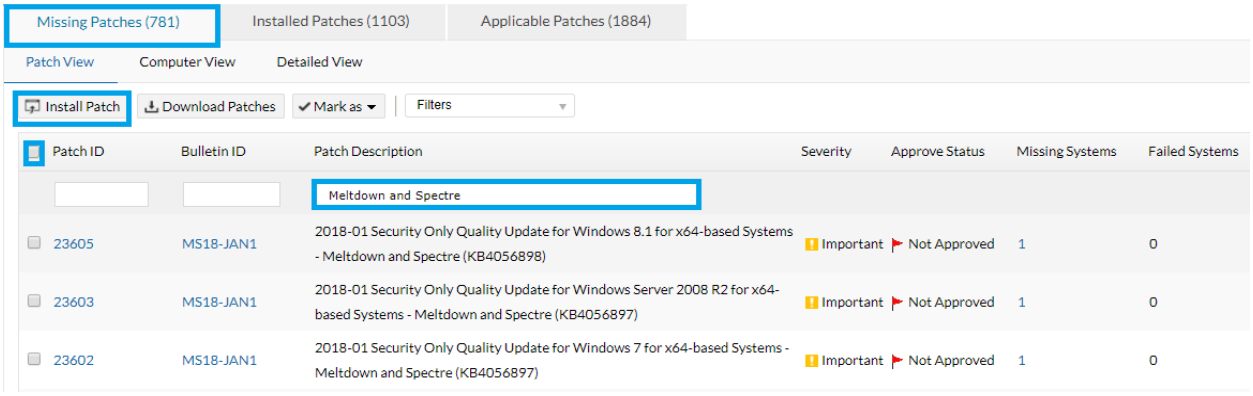
Mitigating Meltdown and Spectre

Even after a year of discovery of Meltdown and Spectre, mitigations are still underway. Installing the microcodes, BIOS updates, driver updates and other necessary software updates mentioned above is a viable short-term fix . Until chip manufacturers can resolve these hardware vulnerabilities, operating system and application patches can help prevent hackers from leveraging Meltdown and Spectre . For enterprises, investing in the right patching solution can reduce the complexity of patching on a large scale and help improve productivity.

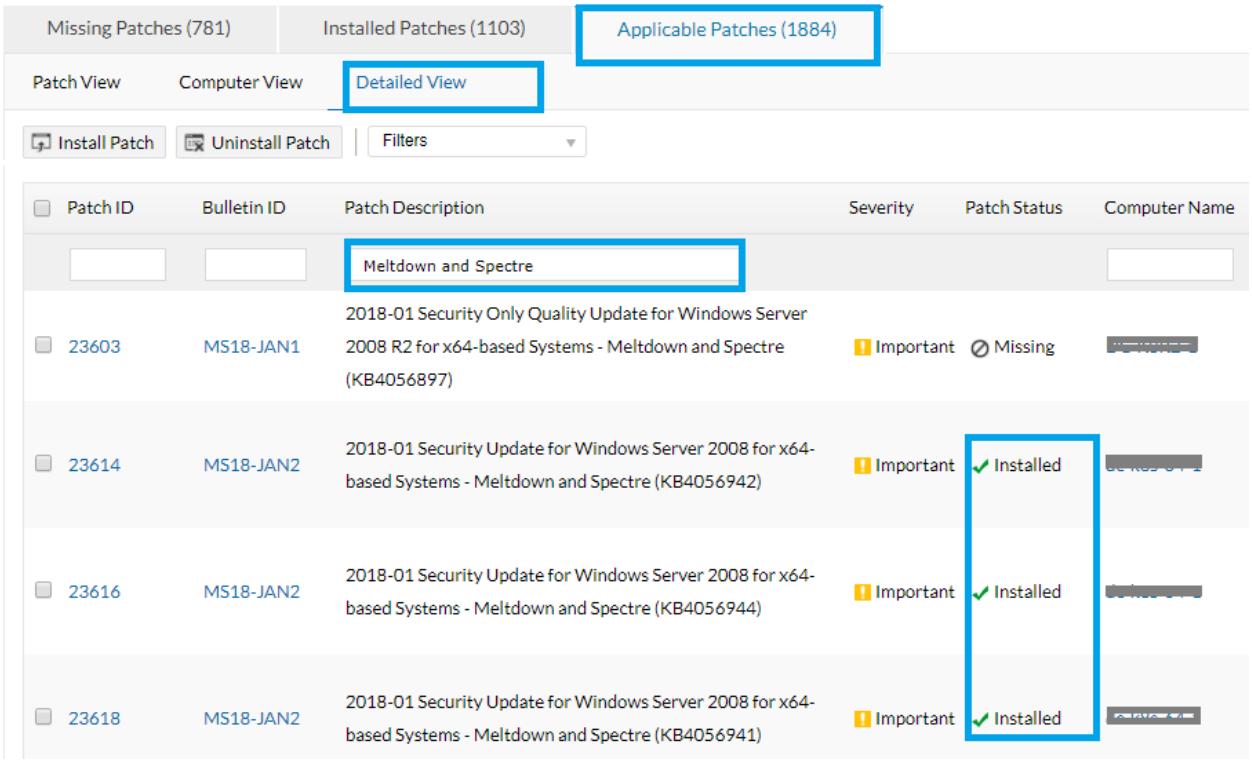
ManageEngine's **Desktop Central** is a complete endpoint management solution that performs automated patch management in enterprises of all sizes. Desktop Central supports over 300 third-party, besides all the OS patches across Windows, Apple, Linux. ManageEngine's patch management solutions typically support patches for all Microsoft's emergency security updates within a day of their release. Meltdown and Spectre patches are rolled out within hours of vendors issuing them. Desktop Central goes beyond just patching, offering other capabilities like software deployment, asset management, license management, remote troubleshooting and a lot more. Desktop Central now also supports deploying patches for hardware components.

Steps below to install all available patches for Meltdown and Spectre using Desktop Central

1. Navigate to the **Patch Mgmt** tab in the Desktop Central console.
2. Click **Update Now** under Update Vulnerability DB.
3. Scan all your systems to identify missing patches.
4. Search for the keywords "**Meltdown**" and "**Spectre**" under the **Patch Description** field. You can also view them under a separate tab called **"Critical Patches**" under Patch Mgmt tab in the console.



5. Select all the missing patches related to Meltdown and Spectre, then click **Install Patch** to deploy them all together.



6. You can also verify their installation status after deployment.

In certain cases, an antivirus software may make unsupported calls to the kernel memory. In such cases, Microsoft patches may not be compatible. It is recommended that the

antivirus be compatible which can be achieved by setting a registry key. The registry key settings can also be configured using Desktop Central

A few best practices to take on hardware vulnerabilities:

1. Attend to processor fixes likes microcodes etc.
2. Automate patching for OS and application updates
3. Apply driver and BIOS updates
4. Monitor your IT assets via IT asset management program
5. Manage privileges for access to various IT management modules like administrator, technicians, Patch Manager etc.

Conclusion

Meltdown and Spectre have resulted in widespread attacks yet; however, , there's a good chance attackers will start leveraging them(or already have) to break through the security systems of enterprises. While Meltdown is less than Spectre, both vulnerabilities leave sensitive data vulnerable—that is, if you don't take precautionary measures.

At this time, all you need to do is keep your computers updated with all patches from Intel, Windows, Apple, ARM, Ubuntu, and all other vendors who have rolled out their own fixes. You don't have to panic, though. ManageEngine can help you mitigate Meltdown and Spectre at your own convenience.