Understanding The Meltdown And Spectre Exploits: Intel, AMD, ARM, And Nvidia

by Paul Alcorn January 4, 2018 at 6:10 AM

After two days of whirlwind developments, we finally have more of a complete picture of the new vulnerabilities that impact processors from the leading vendors. Reports initially surfaced two days ago that Intel's processors are susceptible to a new hardware-based bug that cannot be patched with a mere microcode update. A report from The Register, based in part on a blog post, said that incoming Windows and Linux patches would correct the vulnerability but come with a 5-30% performance loss depending on the workload.

The industry remained silent due to NDAs that were scheduled to expire on January 9, the same date as a round of patches were scheduled to appear. After a day of silence while its stock slumped, Intel issued a statement and claimed the issue is not a hardware bug. Intel also announced that it's

Most Popular

1 Intel Disputes CPU Bug Claims

2 Intel CPU Bug Performance Loss Reports Are Premature

3 Via's Chinese Joint Venture Aims For Competitive Home-Grown X86 SOCs By 2019

working with other titans of the industry, such as AMD and ARM Holdings, to "develop an industry-wide approach to resolve this issue promptly and constructively." AMD has since released a statement and claimed that it has minimal exposure to the primary vulnerability.

The root issues behind the vulnerabilities weren't clearly defined at the time, but a slew of releases from several of the parties involved, along with Google's Project Zero team, have shed light on two new exploits that have served as the catalyst for the recent developments. We'll cover the new exploits below; then we'll get to the updates from Intel, ARM, AMD, and Nvidia.

Performance First

Before we dive into the nuts and bolts, recent tests indicate the patch does not impart a cataclysmic performance loss in most workloads. Phoronix tested the Linux patch, and Computerbase.de tested a patched Windows Insider build.

The good news? Most desktop applications appear to be safe in both Windows 10 and Linux. That includes most workloads that are largely confined to the user space, such as gaming and normal productivity applications. There does appear to be a slowdown to storage I/O operations (2-7%), but for now it's hard to ascertain if that is due to the patch or other kernel updates. The Windows 10 patch was rolled out to the Windows Insider builds in November, and there haven't been reports of performance issues.

The bad news? The patch does incur a performance overhead to some enterprise applications. Phoronix recorded significant performance regressions in the object-relational PostgreSQL database. Redis also suffers a performance loss. Many industry analysts feel the real impacts will come in virtualized environments, but we have yet to see benchmarks. Google has already updated all its cloud infrastructure, which includes its cloud computing services, and we haven't yet heard of significant user backlash due to reduced performance.

Meet Meltdown & Spectre

Google's Project Zero touched off the vulnerability scare when it discovered that it could access data held in the protected kernel memory through two exploits that are now known as Meltdown and Spectre. Google does not believe these exploits have ever been used in the wild, but it's impossible to tell if they have or not.

Meltdown is both easy to execute and easy to fix. This exploit allows applications to read from the protected kernel memory. That ability can allow hackers to read passwords, encryption keys, or other data from the memory. Intel's statement specifically noted that the exploits cannot corrupt, modify, or delete data, but those points are moot if the attacker can access passwords and encryption keys. The biggest concern for data centers and cloud service providers is that the exploit also allows an application resident in one virtual machine to access the memory of another remote virtual machine. This means an attacker could rent an instance on a public cloud and collect information from other virtual machines on the same server.

Researchers have been able to execute a Meltdown exploit only on Intel processors, although ARM has submitted patches to protect itself from the same method of attack. In fact, the attack exploits Intel's out-of-order execution implementation that is present on every Intel processor made since 1995. Researchers discovered Meltdown last year. The exploit is reportedly simple enough that a script kiddie could execute the attack, so a fix is of utmost importance.

Apple already patched this exploit in the MacOS December OSX patch (10.13.2). Windows is also pushing emergency patches out immediately. The Linux kernel has also been patched. These patches do have performance impacts, as we noted above, that largely revolve around how frequently the application issues kernel calls.

The Spectre exploit is much more nefarious and impacts Intel, AMD, and ARM. This exploit can access kernel memory or data from other applications. Researchers contend that fixing this exploit would require a fundamental re-tooling of all processor architectures, so we'll live with the threat of this vulnerability for the foreseeable future. Fortunately, this exploit is extremely hard to execute and requires an elevated level of knowledge of the interior workings of the target processor.

These two exploits are categorized into three variants. Variants 1 and 2 are Spectre, whereas Variant 3 is Meltdown. Intel is vulnerable to all three.

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)

Levels Of Exposure

We reached out to AMD, and the company responded with the following information, which has since been publicly released.

Most notably, AMD claims that is has zero vulnerability to Variant 3 (Meltdown), stating that the patches that are currently being issued for Meltdown do not apply to its processors due to "architectural differences." This is excellent news for AMD, as it therefore has no exposure to the current round of potentially performance-sapping patches. That bodes very well for the company as it reenters the data center with a competitive line of EPYC processors.

The Ryzen desktop processors are also not susceptible to Meltdown. Linus Torvalds has also granted AMD an exemption to the performance penalties incurred by the Linux patch for Meltdown.

AMD is vulnerable to Variant 1, which is a Spectre exploit. As noted above, many contend that Spectre is not likely to see an effective patch any time soon, and some researchers claim the vulnerability exists in every modern processor architecture in existence. They also claim that fixing the issues could require a redesign of fundamental processor architectures. AMD said it has a patch that can mitigate Variant 1 with minimal performance impact and further stated that it has a "near zero risk of exploitation" from Variant 2, which is also a Spectre exploit.

Nvidia also issued a statement regarding the vulnerabilities:

> Nvidia’s core business is GPU computing. We believe our GPU hardware is immune to the reported security issue and are updating our GPU drivers to help mitigate the CPU security issue. As for our SoCs with ARM CPUs, we have analyzed them to determine which are affected and are preparing appropriate mitigations.

ARM Holdings has added a security update to its website that outlines its exposure to the vulnerabilities, and like Intel, it is susceptible to all three variants.

The legal ramifications of these developments could be troublesome. The Law Offices of Howard G. Smith has already announced an investigation on behalf of Intel Corporation investors, and there will likely be more similar developments in the coming weeks. Intel has a history of establishing a reserve to cover pending large-scale hardware replacements, but the company has not disclosed a new fund to deal with the vulnerabilities. The company has also stated that it does not expect any impact to its business.

Intel's statement on the matter specifically says that the exploits are not caused by a "bug" or a "flaw" that is unique to Intel products. Intel also noted that the exploits can "gather sensitive data from computing devices that are operating as designed." These statements likely indicate Intel will defend any potential claims because "the hardware is working correctly." Depending on when these vulnerabilities became known (some claim that Meltdown-type

attacks have been a known entity since 2010), these points may be challenged in court. ARM and other vendors may also face similar challenges.

Intel's CEO, Brian Krzanich, also sold $39 million in stocks in November 2017 (this doesn't include the amount he paid for the stock options). These transaction initially appeared innocuous (and they may be) because Krzanich sold the stock under a 10b5-1(c) plan, which is a pre-planned sale of stocks intended to prevent claims of insider trading. The sale left Krzanich with the Intel-mandated minimum of 250,000 stocks. The sale was pre-planned on October 30. Now, though, MarketWatch claims Intel was made aware of the vulnerability on June 1, which may draw attention to the matter from regulatory officials. Business Insider said a representative for the Securities and Exchange Commission declined to comment on the matter.

Considering the lengthy preparation period, we imagine there will not be any major service disruptions to the cloud service providers. However, we expect more details to come to light concerning performance impacts of the new patches on various workloads. Stay tuned.