Accenture Security

PROCESSOR CHIP DESIGN VULNERABILITIES

DEALING WITH THE THREATS POSED BY **MELTDOWN** AND **SPECTRE**

Meltdown and Spectre are the latest vulnerabilities to raise cybersecurity concerns as the threat of attack grows. On average, organizations suffer two to three focused security breaches each month—attacks they admit could sometimes take years to detect[i]. In the case of Meltdown and Spectre, breaches may be impossible to prevent or detect.

WHAT'S THE STORY?

Meltdown and Spectre represent two vulnerabilities in microprocessor design which leave the world's laptops, desktops, servers, smartphones, other mobile devices and cloud services open to potential attack and abuse. Considering the nature of the vulnerabilities, it is highly unlikely that organizations will be able to detect whether a system has been successfully attacked.

Meltdown is a vulnerability affecting main microprocessor manufacturers with Advanced Micro Devices (AMD) currently being reported as unaffected. Part of the reason that this vulnerability exists is the race for microprocessor performance. To perform as fast as possible, a chip predicts which code it may need to run next. If this predictive assumption is wrong, the chip discards the operations it does not need. Remnants of the "speculative" code—which can include logins, passwords, personally identifiable information (PII) and encryption keys—remain in the memory cache at risk of exploitation. Meltdown enables attackers to execute code that can read this memory and capture the data. Meltdown is relatively easy to exploit, but patches are becoming available to remediate its effects. These patches can degrade processor speed by five to 30 percent according to reports—which will affect cost, load and performance.

Spectre is a flaw in the architecture of microprocessor design making processors from most, if not all, manufacturers vulnerable to attack. Fixing it is difficult and may rely on a new generation of redesigned microprocessors.

Of the two vulnerabilities, Spectre appears more serious, although it is also more difficult to exploit. The fix for Spectre is not simple and will take the industry time to address completely—indeed, the impact could be felt throughout a complete generation of CPU hardware.

WHAT DOES IT MEAN?

With the potential for services to be disrupted, and the difficulties of enforcing patch updates, the overall cost to businesses could be punitive. There are a number of implications:

SECURITY IMPACT

Reading arbitrary kernel memory is dangerous. Potentially, it could lead to the leaking of information, such as keys, passwords, and other sensitive information, including personally identifiable information (PII) and intellectual property (IP). The information obtained from system memory can be used to conduct further attacks and expose vulnerabilities on a range of devices.

From an adversary's point of view, there are various possible tactics, techniques, and procedures (TTPs) to weaponize or operationalize these vulnerabilities, including the following examples:

- One possible attack venue leveraging Spectre would be finding which services are sharing the same cloud hardware and trying to siphon or dump data.
- Because cloud users are unable to implement customized countermeasures to prevent such leaks, there has been an increase in the use of so-called private clouds (that is, organizations that do not rely on popular cloud service providers and choose to host virtualized services within their own data centers). But while organizations may be looking to set up their own clouds, they do not have the expertise of the major cloud providers to help them remain vigilant about security issues. Such cloud infrastructure may be reasonably easy to attack compared with cloud services maintained by the major cloud providers.
- Regarding Meltdown, because it is a non-intrusive kernel reading vulnerability it is currently mitigated only by installing OS vendor patches. However, Accenture Security's iDefense assesses it will not be long before adversaries leverage the vulnerability to gain elevated privileges and remote code execution.

CLOUD-BASED SERVICES

Cloud services are also affected, as multiple virtual machines are often provided on a single physical machine. Spectre can be used to leak hypervisor memory to the user space of a guest virtual machine. An attacker with a presence on a virtual machine in the cloud, for example, could theoretically use a specially crafted

program to access the memory contents of other customers' virtual machines on the same physical system or even the hypervisor itself.

Most blockchain cryptocurrency exchanges, such as Coinbase, also run in the cloud. Considering the recent significant increase in cryptocurrency values, the use of these vulnerabilities on cryptocurrency exchanges may pose a strong potential threat.

COST AND PERFORMANCE

One of the effects of patching these vulnerabilities is an increase in processor utilization. Some reports claim a modest increase of five percent while other reports claim up to a 30 percent increase in processor utilization. This has a direct effect on the cost of a project. Although the performance impact is uncertain, older devices are likely to suffer most and the resultant poor performance costs may have to be absorbed by organizations.

Performance benchmarks are a useful method of comparison in the microprocessor market. Once processor vendors fix the inherent problems with speculative execution, all previous processor performance benchmarks become invalidated. New benchmarks could potentially close the performance gap between processor vendors.

WHAT CAN YOU DO?

Take practical steps today to protect your organization from future malware attacks that may exploit the Meltdown and Spectre vulnerabilities.

- Prioritize patching, especially of virtual machine (VM) software. Both the hypervisor and guest virtual machines.
- Test patches for performance before deploying them to production.
- Increase scrutiny of phishing e-mails that may contain attached executable files.
- Regularly review performance metrics on cloud-based servers looking for unexplained performance degradation.
- Do adequate performance testing, and add more resources as required to arrive at the desired performance level—applying operating system (OS) patches to mitigate the Meltdown attack may degrade performance.
- Take a risk-based review of the un-patchable systems in your estate—given the ubiquity of microprocessors, older systems running critical functions may be most at risk.

TECHNICAL ANALYSIS

The information in this Cyber Advisory is intended to be consumed by administrators and security analysts. Given the inherent nature of threat intelligence, it is based on information gathered and understood at a specific point in time.

This intelligence can be used to help gauge an enterprise's cybersecurity posture against the vulnerabilities referenced in this report.

DESCRIPTION

Multiple vulnerabilities in processors from different manufacturers make it possible for malicious programs to arbitrarily read memory content. Design flaws in Intel, ARM, and AMD microprocessors enable a program in user-space to arbitrarily read the contents of memory, including the contents of kernel memory. The information obtained from system memory can be used to conduct further attacks, such as conducting read and write operations to gain elevated privileges, carrying out a kernel address space layout randomization bypass attack, or breaking out of a virtual machine environment by attacking multiple vulnerabilities.

These vulnerabilities affect laptops, desktops, mobile devices, and cloud services. Cloud services are vulnerable because multiple virtual machines are often stored on a single machine. An attacker with a presence on a virtual machine on the cloud could use a specially crafted application to access the memory contents of other virtual machines on the same physical system.

Google Inc.'s Project Zero initially discovered and reported the vulnerabilities. Independently, other security researchers also discovered these vulnerabilities. The following table maps the names given to these issues by various researchers to their CVE IDs:

- Google Project Zero Variant 1: Spectre Vulnerability: bounds check bypass vulnerability (CVE-2017-5753)
- Google Project Zero Variant 2: Spectre Vulnerability: branch target injection vulnerability (CVE-2017-5715)
- Google Project Zero Variant 3: Meltdown Vulnerability: rogue data cache load vulnerability (CVE-2017-5754)

The attacks for these vulnerabilities can be described as “cache timing side-channel attacks” because the attacks rely on indirectly (hence "side-channel") performing information disclosure attacks by observing the memory cache for clues that reveal the contents of the kernel memory. These attacks can also be described as “speculative execution side-channel attacks” because they require that the vulnerable microprocessor perform certain “speculative execution” of instructions to gain performance.

MELTDOWN

The Meltdown vulnerability (CVE-2017-5754) is used to defeat kernel ASLR (KASLR) and read system memory.

On Linux, the fix for this vulnerability is referred to as the KAISER or "Kernel Page Table Isolation" (KPTI) fix. The fix mitigates the vulnerabilities in the processors by removing the kernel information.

Apple released mitigations for Meltdown in iOS 11.2, macOS 10.13.2, and tvOS 11.2. watchOS did not require mitigation.

iDefense found a publicly available proof-of-concept (PoC) code that exploits this vulnerability on unpatched Windows 10 computers.

Please refer to the iDefense (CVE-2017-5754) vulnerability fundamental for more-technical details.

SPECTRE

The Spectre vulnerability can be used to read arbitrary memory locations of other applications. It has the following two variants:

- iDefense ID: CVE-2017-5715 - Multiple Vendor Microprocessors Branch Target Injection Security Bypass Vulnerability
- iDefense ID: CVE-2017-5753 - Multiple Vendor Microprocessors Bounds Check Security Bypass Vulnerability

The fix for Spectre is not a simple one and will take the industry a long time to address completely.

Please refer to the related iDefense vulnerability fundamentals on CVE-2017-5715 and CVE-2017-5753 for more technical details.

Spectre is the more serious of the two vulnerabilities. It affects all major processors currently on the market. It is harder to exploit and harder to mitigate.

PROCESSOR VENDOR RESPONSES

- AMD - "An Update on AMD Processor Security"
- Intel - "Intel Responds to Security Research Findings"

Intel has released a list of processor names that are vulnerable: "Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method".

- ARM - "Vulnerability of Speculative Processors to Cache Timing Side-Channel Mechanism"

ARM Cortex-A72, Cortex-A57, Cortex-R8, Cortex-A17, Cortex-A15, Cortex-A9, Cortex-R7, Cortex-A75, Cortex-A8, and Cortex-A73 are vulnerable. ARM contained an advisory addressing these issues; however, the domain became unresponsive as of Jan. 4, 2018, at 9 a.m. ET.

- IBM - "Potential Impact on Processors in the POWER family"

IBM's POWER7+, POWER8, and POWER9 platforms will receive firmware updates on Jan. 9, 2018.

IMPORTANT OS VENDOR RESPONSES

MICROSOFT

Microsoft Corp. released out-of-band patches for its Microsoft operating system (OS) during the night of Jan. 3, 2018.

It is crucial to note that Microsoft has identified a compatibility issue with a small number of anti-virus (AV) software products that result in stop errors (also known as blue screen errors) that make the device unable to boot. Therefore, to help prevent stop errors caused by incompatible anti-virus applications, Microsoft is only offering the Windows security updates released on Jan. 3, 2018, to devices running anti-virus software from partners who have confirmed their software is compatible with the January 2018 Windows operating system security update.

Systems which run non-conforming AV and have not set the registry patch, will not only miss the Microsoft security patches for January 2018 but will also miss any further security patches. Hence, it is critical to figure out the installed AV's conformance and the existence of the registry key. Any changes from one AV vendor to another in the future, will require a re-evaluation of the conformance and the registry key's value.

Since Microsoft does not offer a list of affected Anti-Virus vendor names, there is an ongoing effort by Kevin Beaumont on the web.

Furthermore, servers running Microsoft OS will require the manual creation of a registry patch to obtain the security updates related to Meltdown and Spectre.

APPLE

Apple has already released mitigations to help defend against Meltdown in iOS 11.2, macOS 10.13.2, macOS 10.13.3 and tvOS 11.2.

Apple has released mitigations for Spectre 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 will release further mitigations.

LINUX

Linux has reportedly already patched some of the vulnerabilities.

IBM

IBM has stated that patches to its AIX and i operating systems will be available Feb. 12.

IMPORTANT CLOUD PROVIDER RESPONSES

AMAZON WEB SERVICES

As of Jan. 3, 2018, Amazon Web Services (AWS) has reportedly patched most of its instances across the Amazon EC2 fleet and will continue patching throughout the day along with sending maintenance notifications.

Updates and instructions for Amazon Linux are currently available via the AMI repository. Customers with Amazon Linux AMI instances can run the following command to receive the updated package:

- yum update kernel

Updated EC2 Windows AMIs will be provided as Microsoft patches become available. More information on AWS EC2 is available on Amazon's website.

MICROSOFT AZURE

Microsoft reported that the majority of Azure infrastructure has already been updated to address this vulnerability and will begin automatically rebooting the remaining impacted VMs starting at 3:30 pm PT on Jan. 3, 2018.

On Jan. 4, 2018, *The Register* reported that certain customers are reporting problems with their virtual machines, which are struggling to come back online after being updated with the Meltdown patch.

ORACLE

Oracle Corp. has not publicly released any information about its cloud offering, with such announcements often made through its blog on its website or Twitter, with neither indicating anything about its cloud services at this time.

Oracle in its regular patching cycle, will release patches on Tuesday, January 16, 2018. iDefense believes some of the patches released may be related to Meltdown and Spectre.

RESPONSES FROM IMPORTANT WEB BROWSER VENDORS

MICROSOFT IE AND EDGE

Microsoft released patches for Edge and Internet Explorer 11, which reportedly mitigate the vulnerabilities. Microsoft has stated that it may release more patches as additional hardening features.

GOOGLE CHROME

Google suggests that Chrome allows users to enable an optional feature called "Site Isolation" which reportedly mitigates exploitation of these vulnerabilities. Chrome's JavaScript engine, V8, will include mitigations starting with Chrome 64, which will be released on or around Jan. 23, 2018.

GOOGLE ANDROID

Google's Android security update on 1/2/208 patched CVE-2018-13218; this update provides additional protection by reducing access to high-precision timers, which limits side channel attacks on variants of the ARM processor.

MOZILLA FIREFOX

Mozilla released Firefox version 57.0 and 57.0.4 which reportedly mitigates the vulnerabilities. Mozilla plans to release more mitigation methods via new releases.

APPLE SAFARI

Apple has stated that it will release updates to Safari Web browser.

IMPACT

SECURITY

Spectre can be used to leak hypervisor memory to the user space of a guest virtual machine. Reading arbitrary kernel memory is highly dangerous. Potentially, it could lead to the leaking of information, such as keys, passwords, and other sensitive information, including personally identifiable information (PII). Additionally, this works on virtualized hosts and docker containers.

COST AND PERFORMANCE

One of the effects of patching these vulnerabilities is an increase in processor utilization. Some reports claim a modest increase of 5 percent while other reports claim up to a 30 percent increase in processor utilization. This has a direct effect on the cost of a project. Cloud instances, for example, will have to increase the number of compute instances to handle the new utilization.

Of the many processor bugs that Intel has encountered, the 1994 FDIV bug in the Pentium chip was a major one. It cost the company $475 million US in pre-tax earnings. Ever since the discovery of that bug, Intel has been careful about validation before releasing products.

CRYPTOCURRENCY EXCHANGES

Most cryptocurrency exchanges, such as Coinbase, run in the cloud. Considering the recent significant increase in cryptocurrency values, the use of these vulnerabilities on exchanges may pose a strong threat.

FUTURE OF BENCHMARKS

Once processor vendors fix the inherent problems with speculative execution, all previous processor performance benchmarks become invalidated. The new benchmarks could potentially close the performance gap between the two major processor vendors.

ADVERSARY CONSIDERATIONS

POSSIBLE TACTICS, TECHNIQUES AND PROCEDURES (TTPS)

From an adversary's point of view, there are various possible TTPs to weaponize or operationalize these vulnerabilities, including the following examples:

a) One possible attack venue leveraging Spectre would be finding which entities are sharing the same cloud (such as cleared clouds, etc.) and trying to siphon or dump data.

b) Because cloud users can hardly implement customized countermeasures to prevent such leaks, there has been an increase in the use of so-called private clouds (i.e., organizations not relying on popular cloud service providers). Organizations are looking to set up their own clouds but do not have the expertise of major cloud providers to help them remain vigilant about security issues. Such cloud infrastructure may be reasonably easy to attack compared to cloud services maintained by the major cloud providers.

c) Regarding the Meltdown vulnerability, because it is a way to read kernel information and is currently mitigated only by installing OS vendor patches, iDefense assesses it will not be long before adversaries leverage the vulnerability to gain elevated privileges and remote code execution.

iDefense has not noticed an uptick in spam related to these vulnerabilities as of the morning of Jan. 4, 2018.

EMERGING EFFORTS

iDefense analysts have observed discussions regarding the Meltdown and Spectre vulnerabilities on at least one routinely monitored criminal forum. The discussion was initiated by one of the moderators of a popular Russian-language underground forum. On Jan. 4, 2018, the moderator opened the discussion providing links to the following:

- Existing research on the vulnerabilities
- Utility to check for the vulnerabilities
- PoC on GitHub
- PSH script for checking the vulnerabilities

Because all PoCs are concentrated on Intel, the moderator saw an opportunity to exploit these vulnerabilities on platforms other than Intel. Another forum user extended the discussion to include ARM and AMD processors.

Considering the direct mention of exploitation of the vulnerabilities by the moderator, and the opportunistic nature of the criminal underground marketplace, iDefense analysts predict seeing the emergence of malware exploiting these vulnerabilities for sale or hire on the black market in the coming days and weeks. It should be noted that exploits for these vulnerabilities that appear on the black market may not be authentic, as many threat actors may be attempting to capitalize on the vulnerabilities and earn quick money by ripping off unsuspecting buyers who believe they are purchasing legitimate exploits.

News of the vulnerabilities will undoubtedly be posted to underground forums in the coming days and will generate further discussion among threat actors.

FREQUENTLY ASKED QUESTIONS

Q: Can a microcode fix these vulnerabilities?
A: While Meltdown is being mitigated by patches to software, Spectre is being mitigated by fixes at both hardware and software levels. Some vendors, like Google, are mitigating Spectre only at the software level.

Q: Is AMD immune to the vulnerabilities?
A: Not really. AMD is vulnerable to the Spectre attacks, but not to Meltdown attacks.

Q: How often are such serious vulnerabilities discovered in microprocessors?
A: Although the discovery of vulnerabilities in microprocessors is not completely uncommon, vulnerabilities this severe are unusual.

Q: What is KAISER?
A: KAISER is the old name of the patches that are now referred to as Kernel Page Table Isolation (KPTI).

Q: Can we detect successful exploitation?
A: No. Considering the nature of the vulnerabilities, it is highly unlikely that one could detect whether a system has been exploited successfully. There are some ideas on how an ongoing attack can be detected by endpoint detection and response (EDR) solutions.

MITIGATION

iDefense makes the following recommendations regarding these vulnerabilities:

- Apply operating system patches
- Prioritize patching of virtualization hypervisors
- Prioritize patching of Docker host kernels
- Test Linux kernel patches to gauge system performance before deploying them in a production environment, scaling up instance specifications as needed

As referenced, Linux and Windows have patches for Meltdown.

Spectre is harder to mitigate, and any patch for it is a work in progress.

CONTACT US

Kelly Bissell
kelly.bissell@accenture.com

Justin Harvey
justin.harvey@accenture.com

Uwe Kissman
uwe.kissman@accenture.com

Ryan LaSalle
ryan.m.lasalle@accenture.com

Gareth Russell
gareth.russell@accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

About Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

[i] Accenture Security High Performance Security Report 2016