Bulletin d'alerte de sécurité du CSIRT DOCAPOST
Multiples vulnérabilités de fuite d'informations dans des processeurs
CSIRT-DCP-ALE-2018-01

GESTION DU DOCUMENT

Date de la première version :	04/01/2018
Date de la dernière version :	06/02/2018
Version :	1.6
Source :	Service de Lutte Contre La Cybercriminalité (SLCC La Poste) Agence National de la Sécurité des Systèmes d'Information (ANSSI)

RISQUE(S) / IMPACT(S)

Score CVSS

Score de base :	4.0	AV:L / AC:M / Au:S / C:P / I:N / A:N
Score temporel :	3.4	E:POC / RL:OF / RC:C
Score Environmental :	5.1	CDP:ND / TD:H / CR:H / IR:ND / AR:ND

Risque(s)

- Atteinte à la confidentialité des données

Impact(s)

Les vulnérabilités décrites dans cette alerte peuvent impacter tous les systèmes utilisant un processeur vulnérable et donc de façon indépendante du système d'exploitation. Selon les chercheurs à l'origine de la découverte de ces failles, il est ainsi possible d'accéder à l'intégralité de la mémoire physique sur des systèmes Linux et OSX et à une part importante de la mémoire sur un système Windows. On notera que l'impact peut être plus particulièrement important dans des systèmes de ressources partagés de type conteneur (Docker, LXC) où il serait possible depuis un environnement restreint d'accéder à toutes les données présentes sur la machine physique dans lequel s'exécute le conteneur ou encore dans des environnements virtualisés utilisant la para-virtualisation de type Xen.

RESUME DE LA VULNERABILITE OU DE LA MENACE

- **CVE-2017-5753** : Contournement des frontières. Un attaquant local pourrait l'exploiter afin de lire des portions arbitraires de 4GB de la mémoire du noyau via une application utilisateur spécialement conçue. Cette vulnérabilité, due à une lecture mémoire hors des limites dans la fonctionnalité d'optimisation processeur "Branch Prediction", est exploitable par l'attaque Spectre. Cette vulnérabilité existe sous condition que l'interpréteur ou moteur eBPF JIT soit activé par le noyau

- **CVE-2017-5715** : "Branch target injection". Un attaquant en tant qu'invité privilégié (root) dans une machine virtuelle pourrait l'exploiter afin de lire des informations provenant de la mémoire de l'hôte via l'exécution d'une application spécialement formée en mode utilisateur l'invité. Cette vulnérabilité, due à des fuites de mémoire possible dans les caches pour la fonctionnalité d'optimisation processeur "Branch Prediction", est exploitable par l'attaque Spectre.

- **CVE-2017-5754** : "Rogue data cache load". Un attaquant local pourrait l'exploiter afin d'obtenir des informations provenant du noyau via une application spécialement formée en mode utilisateur. Cette vulnérabilité, due à une mauvaise gestion des caches par certains CPU Intel, est exploitable par l'attaque MeltDown.

VECTEUR(S) D'INFECTION(S) / D'ATTAQUE(S)

- Local à la machine
- Navigateurs web

Campagne de pourriels

Le **CERT-FR** constate qu'une campagne de pourriels visant à distribuer des logiciels malveillants a été lancée afin de profiter de la situation autour des vulnérabilités Spectre et Meltdown. Des attaquants se faisant passer pour la Bundesamt für Sicherheit in der Informationstechnik (BSI), l'équivalent allemand de l**ANSSI**, ont envoyé des courriers électroniques invitant leurs destinataires à se rendre sur une copie du site de la BSI. La différence avec le site officiel était une modification de l'alerte concernant les vulnérabilités: l'utilisateur était invité à installer un correctif qui se trouvait être un logiciel malveillant.

Le **CSIRT DOCAPOST** rappelle de faire preuve de la plus grande vigilance quant à l'ouverture des courriers électroniques ainsi que d'installer les correctifs de sécurité dans les plus brefs délais, et ce uniquement depuis les sources officielles des éditeurs.

SYSTÈME(S) AFFECTÉ(S)

- Voir Section : **Documentations et Informations Techniques**

RESUME

Plusieurs vulnérabilités ont été identifiées dans différents processeurs modernes d'Intel, ARM et AMD. Ces vulnérabilités ont été découvertes et exploitées dans le cadre de plusieurs recherches relatives aux attaques par canaux auxiliaire d'exécution spéculative, ces attaques sont les suivantes :

- Meltdown : Tous les CPU, trois preuves de concept privé existent (Google Project Zero)
- Spectre : Intel, ARM et AMD, une preuve de concept privé existe (Google Project Zero).

Mise à jour du 23/01/2018 : modification des recommandations suite au communiqué d'Intel (cf. **Documentations et Informations Techniques**)

VULNÉRABILITÉ MELTDOWN

Les processeurs modernes intègrent plusieurs fonctionnalités visant à améliorer leurs performances. Parmi celles-ci, l'exécution dis out-of-order permet d'exécuter les instructions d'un programme en fonction de la disponibilité des ressources de calculs et plus nécessairement de façon séquentielle. Une faiblesse de ce mécanisme peut cependant conduire à l'exécution d'une instruction sans que le niveau de privilèges requis ne soit correctement vérifié au préalable. Bien que le résultat de l'exécution d'une telle instruction ne soit pas validé par la suite il peut être possible de récupérer l'information en utilisant une attaque par canaux cachés.

La vulnérabilité CVE-2017-5754 permet d'exploiter une fonctionnalité présente dans plusieurs architectures de processeurs modernes afin d'accéder en lecture à des zones mémoires d'un système autrement non accessibles sans des privilèges élevés. En particulier, l'exploitation de cette vulnérabilité permet d'accéder depuis un programme s'exécutant en mode utilisateur à la mémoire du système en mode noyau. Cela peut conduire à des fuites de données sensibles présentes en mémoire et peut inclure des informations d'autres programmes ou encore des clés de chiffrement. Cette fuite d'informations peut aussi être mise en œuvre pour faciliter la compromission d'un système.

VULNÉRABILITÉ SPECTRE

L'exécution spéculative est une seconde technique d'optimisation utilisée par les processeurs modernes. Lorsqu'un processeur est en attente d'une information de la part de la mémoire centrale, il peut continuer à exécuter des instructions de manière probabiliste afin de ne pas gâcher des cycles. Quand cette information arrive, le processeur vérifie la cohérence de son résultat anticipé. Dans le meilleur cas, il a gagné du temps car il a correctement prédit l'information. Dans le pire cas, il n'en a pas perdu car il reprend l'exécution de ses instructions avec la bonne information. Si le contenu des registres sont remis à leurs valeurs initiales, ce n'est pas le cas du cache. L'exemple donné dans l'article décrivant Spectre est le suivant:

```
if (x < array1_size)
y = array2[array1[x] * 256];
```

Selon les bonnes pratiques, on teste si l'index est bien dans les limites du tableau avant d'y accéder. Or, si l'on a déjà demandé plusieurs fois d'accéder au tableau avec des valeurs légitimes, le processeur partira du principe que les valeurs demandées seront légitimes dans le cadre de l'exécution spéculative. Un attaquant pourra alors fournir une donnée erronée afin de provoquer un débordement de tampon. Une fois que le processeur exécutera réellement l'instruction, il se rendra compte de l'erreur, cependant le résultat de la lecture interdite restera dans le cache. Il faut ensuite récupérer cette information, ce qui n'est pas trivial.

Une autre manière d'exploiter Spectre est de forcer l'exécution spéculative à partir d'un autre processus. Le cas de figure le plus probable étant un hôte tentant d'obtenir des informations de la part de l'hyperviseur. Cette technique est la plus difficile à exploiter, mais également la plus difficile à contourner.

CONTRE(S) MESURE(S)

- Voir Section : **Documentations et Informations Techniques**

MESURE(S) REACTIVE(S)

- Mise à jour des postes de travail Windows et Linux
- Mise à jour des hyperviseurs afin de limiter les rebonds de machines virtuelles à machines virtuelles
- Mise à jour des serveurs ayant un rôle d'administration

Attention : Pour les serveurs d'applications il est préférable d'effectuer des tests de performances

- Voir Section : **Documentations et Informations Techniques**

IOC

- **N.C**

DOCUMENTATIONS ET INFORMATIONS TECHNIQUES

CERT Announce

- CERT/CC: Vulnerability Note VU#584653 - CPU hardware vulnerable to side-channel attacks
- US-CERT: TA18-004A - Meltdown and Spectre Side-Channel Vulnerability Guidance
- CERT-EU: Security Advisory 2018-001 - Meltdown and Spectre Critical Vulnerabilities
- NCSC-UK: Meltdown and Spectre guidance
- CERT-FR: CERTFR-2018-ALE-001 - Multiples vulnérabilités de fuite d'informations dans des processeurs
- CERT Nazionale: Moderni processori vulnerabili ad attacchi side-channel(italian only)
- CERT-PA: Meltdown e Spectre, vulnerabiliti sui microprocessori mettono potenzialmente a rischio informazioni sensibili(Italian only)

- CERT-GARR: ALERT GCSA-18001 - Vulnerability Meltdown e Spectre(italian only]
- SingCERT: Alert on Security Flaws Found in Central Processing Units (CPUs) [1]
- CERT.BE: Architectural Design Flaws Central Processor Unit (CPU) [2]
- CERT-IS: Alvarlegur Çôryggisgalli Çð ÇôrgjÇôrvum - Meltdown/Spectre (Icelandic only]
- MyCERT: MA-691.012018: Alert - CPU Hardware Side-Channel Attacks Vulnerability
- CERT-BUND:buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Meltdown_Spectre_Sicherheitsluecke_10012018.html Prozessor-Schwachstellen: Spectre und Meltdown (German only)

Spectre & Meltdown Checkers

(Use at your own risk)

- Linux: Stéphane Lesimple put together "a simple shell script to tell if your Linux installation is vulnerable against the 3" "speculative execution" "CVEs."]
- Linux: Red Hat Check Script Get the latest version from the diagnose tab of the main Red Hat vulnerability article.]
- Linux: Debian Spectre-Meltdown Checker Spectre & Meltdown vulnerability/mitigation checker available in stretch-backports.
- Microsoft Windows: See the #windows section in this document containing the link to the official Powershell script.

PoCs

- In a recent tweet Moritz Lipp (Graz University of Technology has announced the release of their PoC implementations for Meltdown.
- GitHub repository
- In a recent tweet Jann Horn (Google's Project Zero has announced that the PoC code referenced in their recent blogpost about CPUs is now public.
- The LSDS group at Imperial College London has published sample code demonstrating a Spectre-like attack against an Intel SGX enclave.
- Dag-Erling published a Meltdown PoC for FreeBSD.

Antiviruses

Some Antiviruses do things that break when installing the Windows patches, therefore Microsoft doesn't automatically install the patches on those systems.

Vendor
overview: https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?usp=sharing&sle=true

- Trend Micro: Important Information for Trend Micro Solutions and Microsoft January 2018 Security Updates Meltdown and Spectre
- Emsisoft: Chip vulnerabilities and Emsisoft: What you need to know
- Sophos: Advisory - Kernel memory issue affecting multiple OS aka F..CKWIT, KAISER, KPTI, Meltdown & Spectre
- Webroot: Microsoft Patch Release - Wednesday, January 3, 2018
- McAfee: Decyphering the Noise Around Meltdown and Spectre and Meltdown and Spectre Microsoft update (January 3, 2018) compatibility issue with anti-virus products
- Kaspersky: Compatibility of Kaspersky Lab solutions with the Microsoft Security update of January 9, 2018
- ESET: Meltdown & Spectre: How to protect yourself from these CPU security flaws
- Avira: With our latest product update 15.0.34.17 Avira Antivirus Free, Avira Antivirus Pro and Avira Antivirus Server are compatible with the Microsoft update
- Symantec: Meltdown and Spectre: Are Symantec Products Affected?
- Avast: Meltdown and Spectre: Yes, your device is likely vulnerable
- eScan: Meltdown and Spectre CPU Vulnerabilities
- Bitdefender: Meltdown and Spectre: decades-old CPU design flaws put businesses at risk

Linux upstream kernel

Kernel Page Table Isolation is a mitigation in the Linux Kernel, originally named KAISER.

- Version 4.14.11 contains KPTI.
- Version 4.15-rc6 contains KPTI.
- Longterm support kernels Version 4.9.75 and 4.4.110 [https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.110contain KPTI backports.

Noteworthy

- Comment by kernel developer Andrew Lutomirski [https://news.ycombinator.com/item?id=16087736 that pre-4.14 kernels got an earlier version of KPTI and may contain bugs .
- Explanation of PCID which will reduce performance impact of KPTI on newer kernels.

minipli patches

minipli is an unofficial fork of the former grsecurity patches (original grsecurity is no longer publicly available . minipli is based on the longterm kernel 4.9, which supports KPTI since 4.9.75, yet the patchset isn't ported yet.

- Bug report with discussion about backporting KPTI

Android

- Fixed with Android Security Bulletin January 2018.

Windows

- Microsoft Advisory
- Windows Server Guidanceand Windows Client Guidance [https://support.microsoft.com/en-gb/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe . Note: both links include a Powershell tool to query the status of Windows mitigations for CVE-2017-5715 (branch target injection and CVE-2017-5754 (rogue data cache load .
- Protecting guest virtual machines from CVE-2017-5715 (branch target injection [https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/CVE-2017-5715-and-hyper-v-vms
- Understanding the performance impact of Spectre and Meltdown mitigations on Windows Systems
- Spectre mitigations in MSVC

Update - Tue 9 Jan 09:00 UTC

Microsoft has reports of some customers with AMD devices getting into an unbootable state after installing this KB . To prevent this issue, Microsoft will temporarily pause Windows OS updates to devices with impacted AMD processors (older CPUs, eg. Athlon and Sempron at this time. Microsoft is working with AMD to resolve this issue and resume Windows OS security updates to the affected AMD devices via Windows Update and WSUS as soon as possible. If you have experienced an unbootable state or for more information see KB4073707. For AMD specific information please contact AMD.

Update - Sat 27 Jan

- Update to Disable Mitigation against Spectre, Variant 2

Apple

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

- Official statement

Update - Mon 8 Jan 18:00 UTC

Apple has released security improvements to Safari and WebKit to mitigate the effects of Spectre (CVE-2017-5753 and CVE-2017-5715) :

- macOS High Sierra 10.13.2 Supplemental Update
- Safari 11.0.2for Mac OS X El Capitan 10.11.6 and macOS Sierra 10.12.6
- iOS 11.2.2 updatefor iPhone and iPad

Update - Sun 7 Jan 2018, 9:00 UTC

Based on the Apple's response posted here Meltdown (CVE-2017-5754) is currently only addressed in iOS 11.2, macOS 10.13.2, and tvOS 11.2. Apple cannot say at this time if there will be updates to OS versions prior to the ones listed in their article at this time. The same can be said for Spectre (CVE-2017-5753 and CVE-2017-5715) and any updates for Safari. This means that at this given time there are NO patches for 10.11.x (El Capitan) or 10.12.x (Sierra).

Linux distributions

- Red Hat Advisory
- Speculative Execution Exploit Performance Impacts - Describing the performance impacts to security patches for CVE-2017-5754 CVE-2017-5753 and CVE-2017-5715
- Red Hat Check Script - Get the latest version from the diagnose tab of the main Red Hat vulnerability article.
- CentOS:
  - 7 :
    - CESA-2018:0007 (kernel)
    - CESA-2018:0012 (microcode_ctl)
    - CESA-2018:0014 (linux-firmware)
    - CESA-2018:0023 (qemu-kvm)
    - CESA-2018:0029 (libvirt)
  - 6 :
    - CESA-2018:0008(kernel)
    - CESA-2018:0013 (microcode_ctl)
    - CESA-2018:0024 (qemu-kvm)
    - CESA-2018:0030 (libvirt)
  - Fedora - Fixed in :
    - FEDORA-2018-8ed5eff2c0 (Fedora 26)
    - FEDORA-2018-22d5fa8a90 (Fedora 27)

Update - Wed 10 Jan 2018, 08:00 UTC

- Fedora has pushed to **testing** new microcode_ctl packages for F26 FEDORA-2018-6b319763ab and F27 FEDORA-2018-7e17849364. They contain the update to upstream 2.1-15.20180108 and include fix for Spectre.
- Ubuntu (tl subsequent patches for *Spectre* are coming in the future before the kernels are pushed to official release branch dr: Patches for Meltdown now available

The first set of updates for 14.04 / 16.04 was broken on some systems, please make sure you update to the very latest kernel packages and avoid the broken ones.

Update - Sun 7 Jan 2018, 22:00 UTC

Release candidate kernels 4.4.x (Trusty HWE / Xenial GA are now publicly available from a and 4.13.x (Xenial HWE-edge / Artful GA / Artful HWE dedicated Launchpad PPA and currently contain patches for CVE-2017-5754 *aka Meltdown*, with support only some architactures. Support for a broader array of architectures and patches for CVE-2017-5715 and CVE-2017-5753 *aka Spectre* are expected in the near future.

After some testing, the patched kernels will be pushed to the main release branch.

Update - Mon 8 Jan 2018, 16:00 UTC

Canonical Ltd. announced that, in order to speed up the patching process for all supported distribution versions and branches, the 4.10.x *Xenial HWE* kernel will be migrated early to version 4.13.x, thus leaving no supported kernel branch exposed to vulnerabilities. The migration will occur concurrently to the push of patched kernels to the main distribution repositories. In addition, Ubuntu 17.04, aka *Zesty Zapus*, will reach End Of Life on Sat 13 Jan 2018 and will not receive any kind kernel patch support.

- Ubuntu Wiki SecurityTeam KnowledgeBase
- Ubuntu Insights blog : Ubuntu Updates for the Meltdown / Spectre Vulnerabilities
- 17.10: USN-3523-1
- 16.04: USN-3522-1
- 14.04: USN-3522-2
- 16.04/regression: USN-3522-3
- 14.04/regression: USN-3522-4
- "Details about CVE-2017-5753 (variant 1), akaSpectre
- "Details about CVE-2017-5715 (variant 2), aka Spectre
- "Details about CVE-2017-5754 (variant 3), aka Meltdown
- Debian: Meltdown fixed in :
  - Stretch 4.9.65-3+deb9u2 : DSA-4078-1
  - Jessie 3.16.51-3+deb8u1 : DSA-4082-1
  - Wheezy 3.2.96-3 : DLA-1232-1

- "Details about CVE-2017-5753 (variant 1), aka Spectre
- "Details about CVE-2017-5715 (variant 2), aka Spectre
- "Details about CVE-2017-5754 (variant 3), aka Meltdown

- Suse Linux : SUSE Advisory

- Scientific Linux:
  - 7 :
    - SLSA-2018:0007-1 (kernel)
    - SLSA-2018:0012-1 (microcode_ctl)
    - SLSA-2018:0014-1 (linux-firmware

  - 6 :
    - SLSA-2018:0008-1 (kernel)
    - [https://www.scientificlinux.org/category/sl-errata/slsa-20180013-1/ SLSA-2018:0013-1) (microcode_ctl)

- CoreOS Container Linux: Fixes for Meltdown are available in all release channels now (Alpha 1649.0.0, Beta 1632.1.0, Stable 1576.5.0 Auto-updated systems will receive the releases containing the patch on 2017-01-08. Spectre patches are still WIP.

- NixOS: According to #33414 KPTI is in nixpkgs since 1e129a3
- Arch Linux Advisory

- Gentoo:
  - Gentoo Wiki : Project:Security/Vulnerabilities/Meltdown and Spectre
    - Bugtracker - Bug#643228 - Security Tracking Bug

- Oracle Linux (ELSA Security Advisory :
  - Details about CVE-2017-5753 (variant 1) aka Spectre
  - Details about CVE-2017-5715 (variant 2) aka Spectre
  - Details about CVE-2017-5754 (variant 3) aka Meltdown

- CloudLinux: Intel CPU Bug - Meltdown and Spectre - KernelCare and CloudLinux

- Parrot Security OS: meltdown/spectre security patches

- Tails: Tails 3.4 has been released . It contains the fix for Meltdown and partial mitigation for Spectre.
- Manjaro: Detail about Kernel Page-Table Isolation patched with stable update 2018-01-05

FreeBSD

- [https://lists.freebsd.org/pipermail/freebsd-security/2018-January/009719.html Statement

Virtualization

- XEN - XSA-254 and Xen Project Spectre/Meltdown FAQ no patches yet
- QEMU - unofficial patch published here official blog post discussion on qemu-devel

- VMware :
  - vSphere status is tracked in KB52245
    - VMSA-2018-0004
    - Update 01/13/18: All of the ESXi patches associated with VMSA-2018-0004 have been PULLED from the online repository after Intel notified VMware of faulty microcode updates for certain Haswell/Broadwell CPUs. Please see https://kb.vmware.com/s/article/52345 for affected systems & workaround for those applied microcode update until new updates are available from Intel.
    - VMware currently advises patching to the levels provided in [https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html VMSA-2018-0002 .
  - VMware Appliance status is tracked in KB52264

- Red Hat Enterprise Virtualization - Impacts of CVE-2017-5754, CVE-2017-5753, and CVE-2017-5715 to Red Hat Virtualization products

- Citrix XenServer - Citrix XenServer Multiple Security Updates

- Nutanix:
    - Update - Wed 31 Jan 2018**
    - New Nutanix Security Advisory #0007 v9 - Nutanix Side-Channel Speculative Execution Vulnerabilities
  - Update - Wed 17 Jan 2018**
    - New Nutanix Security Advisory #0007 v7 - Nutanix Side-Channel Speculative Execution Vulnerabilities

  - Update - Mon 8 Jan 2018**
    - New Nutanix Security Advisory #0007 v2 - Nutanix Side-Channel Speculative Execution Vulnerabilities
    - Nutanix Security Advisory #0007 v1 Nutanix Side-Channel Speculative Execution Vulnerabilities

- Virtuozzo - Virtuozzo Addresses Intel Bug Questions

- KVM: **Update - Tue 9 Jan 07:50 UTC** - Paolo Bonzini, KVM developer, posted in a tweetthe following status update for CVE-2017-5715 (Spectre) :
  - Already in Linus's tree: clearing registers on vmexit
  - First wave of KVM fixes here: https://marc.info/?l=kvm&m=151543506500957&w=2
  - He is also mentioning that a full solution will require all the Linux parts to be agreed upon, but this will unblock the QEMU updates

Browsers

- Mozilla: Mitigations landing for new class of timing attack blog post
  - Security Advisory 2018-01
  - Firefox mitigation update 57.0.4

- Chrome: Actions Required to Mitigate Speculative Side-Channel Attack Techniques

- Microsoft Edge: Mitigating speculative execution side-channel attacks in Microsoft Edge and Internet Explorer

- Webkit : (open source browser engine What Spectre and Meltdown Mean For WebKit)

- Brave Browser: New desktop release just out 0.19.131 with various security enhancements, including Strict Site Isolation support.
  - Release Notes

Update Mon 8 Jan 2018, 13:00 UTC

Tencent's Xuanwu Lab has released a web-based tool]that can detect whether your browser is vulnerable to Spectre Attack and can be easily exploited. Official tweet

Cloud Providers

- Amazon AWS: Processor Speculative Execution Research Disclosure
- Google Cloud: Google Mitigations Against CPU Speculative Execution Attack Methods
- Microsoft Azure: Securing Azure customers from CPU vulnerability
- DigitalOcean: A Message About Intel Security Findings
- Scaleway/Online: Spectre and Meltdown vulnerabilities status
- Linode: CPU Vulnerabilities: Meltdown & Spectre
- Rackspace: Rackspace is Tracking Vulnerabilities Affecting Processors by Intel, AMD and ARM
- OVH:
  - bug impacting x86-64 CPU : Meltdown/Spectre OVH fully mobilised (en)
  - Vunérabilités Meltdown/Spectre affectant les CPU x86-64 : OVH pleinement mobilisé (fr)
    - Octave Klaba's (OVH CEO Twitter thread)
- Vultr: Intel CPU Vulnerability Alert
- Hetzner: Spectre and Meltdown
- UpCloud: Information regarding the Intel CPU vulnerability Meltdown
- Heroku: Meltdown and Spectre Security Update
- Alibaba Cloud: Intel Processor Meltdown and Specter Security Vulnerability Bulletin
- Zscaler: Meltdown and Spectre vulnerabilities : What you need to know
- Gandi: Meltdown and Spectre vulnerabilities

Chip Manufacturers / HW Vendors

- Intel: INTEL-SA-00088 - Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method] Intel Analysis of Speculative

Execution Side Channels Whitepaper Intel Issues Updates to Protect Systems from Security Exploits Firmware Updates and Initial Performance Data for Data Center Systems Root Cause of Reboot Issue Identified Updated Guidance for Customers and Partners

- AMD: An Update on AMD Processor Security
- ARM: Security Update
- Arista: Security Advisories
- Raspberry Pi: Why Raspberry Pi isn't vulnerable to Spectre or Meltdown
- NVIDIA: Security Notice: Speculative Side Channels
  - NVIDIA Shield Tablet Security Updates

  - NVIDIA Shield TV Security Updates
  - NVIDIA GPU Display Driver Security Updates
  - NVIDIA Tegra Jetson TX2 L4T Security Updates
  - NVIDIA Tegra Jetson TX1 L4T and Jetson TK1 L4T Security Updates
- Lenovo: LEN-18282 - Reading Privileged Memory with a Side Channel
- IBM: Architectural Design Flaws Central Processor Unit (CPU), Potential Impact on Processors in the POWER family
- Huawei: huawei-sn-20180104-01 - Statement on the Media Disclosure of a Security Vulnerability in the Intel CPU Architecture Design
- F5: K91229003 - Side-channel processor vulnerabilities CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754
- Cisco CPU Side-Channel Information Disclosure Vulnerabilities
- Fortigate: CPU hardware vulnerable to Meltdown and Spectre attacks
- Cumulus Linux: Meltdown and Spectre: Modern CPU Vulnerabilities
- Check Point: Check Point Response to Meltdown and Spectre CVE-2017-5753, CVE-2017-5715, CVE-2017-5754
- Palo Alto Networks: Information about Meltdown and Spectre findings PAN-SA-2018-0001
- HP Enterprise: Side Channel Analysis Method Allows Improper Information Disclosure in Microprocessors CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, HPESBHF03805 Certain HPE products using Microprocessors from Intel, AMD, and ARM, with Speculative Execution, Elevation of Privilege and Information Disclosure
- Juniper: 2018-01 Out of Cycle Security Bulletin: Meltdown & Spectre: CPU Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method Meltdown & Spectre: Modern CPU vulnerabilities
- Infoblox: #7346: Spectre/Meltdown Vulnerabilities - CVE-2017-5715, CVE-2017-5753, CVE-2017-5754(Login required)
- FireEye: FireEye Notice for CVE-2017-5754, CVE-2017-5753, and CVE-2017-5715 Meltdown• and Spectre• vulnerabilities, Community Protection Event (CPE : CPU Security Flaws) Spectre/Meltdown (Login required]
- Symantec: Meltdown and Spectre: Are Symantec Products Affected?
- Dell: : Impact on Dell products Microprocessor Side-Channel Vulnerabilities CVE-2017-5715, CVE-2017-5753, CVE-2017-5754
- Dell EMC: Impact on Dell EMC products (Dell Enterprise Servers, Storage and Networking Microprocessor Side-Channel Attacks (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)
- NetApp: NTAP-20180104-0001 - Processor Speculated Execution Vulnerabilities in NetApp Products
- ASUS: ASUS Motherboards Microcode Update for Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method
- Aruba Networks: ARUBA-PSA-2018-001 - Unauthorized Memory Disclosure through CPU Side-Channel Attacks
- Pure Storage: Advisory (login required)
- Supermicro: Security Vulnerabilities Regarding Side Channel Speculative Execution and Indirect Branch Prediction Information Disclosure
- A10 Networks: SPECTRE/MELTDOWN - CVE-2017-5715/5753/5754
- Avaya: Recent Potential CPU Vulnerabilities: Meltdown and Spectre
- RSA: Impact on RSA products 000035890 - Microprocessor Side-Channel Attacks CVE-2017-5715, CVE-2017-5753, CVE-2017-5754 (login required)
- Fujitsu: CPU hardware vulnerable to side-channel attacks 6 SPARC server models listed as t.b.d. p.9
- Veritas Appliance: Veritas Appliance Statement on Meltdown and Spectre
- Polycom: Security Advisory Relating to the Speculative Execution Vulnerabilities with some microprocessors
- Sonicwall: Meltdown and Spectre Vulnerabilities: A SonicWall Alert
- Aerohive Networks: Aerohive's response to Meltdown and Spectre
- Barracuda Networks: Security Advisory
- Netgate: An update on Meltdown and Spectre
- Silver Peak: Security Advisory
- Arbor Networks: Security Advisory(requires support login)
- Extreme Networks:
  - VN 2018-001 CVE-2017-5715, CVE-2017-5753 - Spectre
  - VN 2018-002 CVE-2017-5754 - Meltdown

- KEMP Technologies: Meltdown And Spectre CVE-2017-5754 & CVE-2017-5753
- Pulse Secure: CVE-2017-5715 (Branch Target Injection) AKA Spectre KB43597 - Impact of CVE-2017-5753 (Bounds Check bypass) AKA Spectre and CVE-2017-5754 Meltdown on Pulse Secure Products
- Nokia: Security Advisory(requires Nokia OLCS login)
- Riverbed: Meltdown/Spectre: Side Channel Attacks against X86 hardware and Linux Kernel(requires Riverbed Support Account)
- Acer: Meltdown and Spectre security vulnerabilities
- Asus: ASUS Update on Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method
- Gigabyte: BIOS update for Side Channel Analysis Security issue Mitigations
- Panasonic: Security information of vulnerability by Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method
- MSI: MSI pushes out motherboard BIOS updates to tackle recent security vulnerabilities
- Toshiba: Intel, AMD & Microsoft Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method Security Vulnerabilities
- Vaio: Side Channel Analysis (japanese only)
- HP: HPSBHF03573 rev. 4 - Side-Channel Analysis Method

CPU microcode

- Update - Wed 17 Jan 8:30 UTC
  - Red Hat is currently recommending that subscribers contact their CPU OEM vendor to download the latest microcode/firmware. Red Hat is no longer providing microcode to address Spectre variant 2, due to instabilities that are causing systems to not boot. More details can be found in this article(subscription required)

- Update - Tue 9 Jan 21:50 UTC
  - Latest Intel microcode update (released 1/8/2018 is 20180108. According to its release notes:

```
-- Updates upon 20171117 release --
"IVT C0         (06-3e-04:ed"]428->42a
"SKL-U/Y D0             (06-4e-03:c0"]ba->c2
"BDW-U/Y E/F            (06-3d-04:c0"]25->28
"HSW-ULT Cx/Dx          (06-45-01:72"]20->21
"Crystalwell Cx (06-46-01:32"]17->18
"BDW-H E/G              (06-47-01:22"]17->1b
"HSX-EX E0              (06-3f-04:80"]0f->10
"SKL-H/S R0             (06-5e-03:36"]ba->c2
"HSW Cx/Dx              (06-3c-03:32"]22->23
"HSX C0         (06-3f-02:6f"]3a->3b
"BDX-DE V0/V1           (06-56-02:10"]0f->14
"BDX-DE V2              (06-56-03:10"]700000d->7000011
"KBL-U/Y H0             (06-8e-09:c0"]62->80
"KBL Y0 / CFL D0        (06-8e-0a:c0"]70->80
"KBL-H/S B0             (06-9e-09:2a"]5e->80
"CFL U0         (06-9e-0a:22"]70->80
"CFL B0         (06-9e-0b:02"]72->80
"SKX H0         (06-55-04:b7"]2000035->200003c
```

```
"GLK B0         (06-7a-01:01"]1e->22
```

Update - Thu 4 Jan 2018, 15:30 UTC

It seems that the new Intel microcode archive (2017-12-15) provided with the latest Red Hat microcode_ctl update includes three new files: 06-3f-02, 06-4f-01, 06-55-04.

Based on what we know: 1. it adds one new CPUID and two MSR for the variant of Spectre that uses indirect branches 2. it forces LFENCE to terminate the execution of all previous instructions, thus having the desired effect for the variant of Spectre that uses conditional branches (out-of-bounds-bypass)

Those IDs belong to the following processor microarchitectures: Haswell, Broadwell, Skylake official reference

Update - Thu 4 Jan 2018, 16:30 UTC

Regarding AMD's microcode update: it seems to be only for EPYC (maybe Ryzen, not sure! . It uses a different bit than Intel's in the CPUID. It is also for Spectre with indirect branches. Previous microprocessors resolved it with a chicken bit. Please note that the same solution implemented at kernel level works for both Intel and AMD. and it only adds one of the two MSRs (IA32_PRED_CMD

Update - Fri 5 Jan 2018, 03:35 UTC

Debian Project package maintainers released an "updated version of the intel-microcode package (version 2017-12-15) for the Sid (unstable branch olny). Upon inspection, it seems to contain the same microcode additions observed in the Red Hat microcode_ctl update of Thu 4 Jan 2018, 15:30 UTC.

The package in compatible with all Debian-based distributions that support post-boot microcode updates.

RDBMS

- SQL Server: SQL Server Guidance to protect against speculative execution side-channel vulnerabilities

NOSQL

- Elastic stack: Performance Impact of Meltdown on Elasticsearch Elastic Cloud and Meltdown
- Couchbase: Speculative Execution Processor Vulnerabilities Meltdown and Spectre: What you need to know
- ScyllaDB: The Cost of Avoiding a Meltdown
- Redis Enterprise: Securing Redis Enterprise from Meltdown and Spectre Vulnerabilities
- Redis:
  - Meltdown fix impact on Redis performances in virtualized environments

Embedded Devices

- Synology: Synology-SA-18:01 Meltdown and Spectre Attacks
- Opengear: CVE-2017-5754, CVE-2017-5715, CVE-2017-5753 - Meltdown and Spectre CPU Vulnerabilities
- QNAP: NAS-201801-08 - Security Advisory for Speculative Execution Vulnerabilities in Processors

Compilers

- Google's Retpoline: a software construct for preventing branch-target-injection](technical write-up
- LLVM: An implementation is under review for official merge here
- GCC: An implementation for GCC is available here