


S'inscrire - Se connecter

ACTUALITES
ARTICLES
PRIX
FORUM
BASE OVERCLOCKING
PC HARDWARE.FR
SHOPOK

Découvrez notre gamme de PC de bureau : Office Family Gaming Power Gaming Power User

AMD A-Series AMD FX ASUS Core i3  
Core i5 Core i7 Fermi Haswell  
LGA 1151 LGA 1155 LGA 2011  
Pilotes GeForce Radeon HD 7970  
Skylake USB 3



**La publicité est une source de revenus importante pour HARDWARE.FR**  
**Si vous appréciez notre contenu, désactivez Adblock sur HARDWARE.FR**  
**Merci !**

## Un bug de sécurité coûteux côté serveur chez Intel

Tag : Intel;

Publié le 03/01/2018 à 13:41 par Guillaume Louel

     (423) Réactions

Des chercheurs semblent avoir détecté une vulnérabilité assez importante dans les CPU modernes, qui ne concernerait, c'est encore spéculatif, que les processeurs Intel. Les informations autour de ce bug sont assez limitées, les méthodes de mitigations sont connues mais pas exactement les méthodes d'attaques qui restent sous embargo.

Tout semble partir de [ce blog datant de juillet dernier](#) qui décrit une tentative (a première vue ratée) d'accéder à la mémoire protégée (la mémoire utilisée par le noyau/kernel) à partir du mode utilisateur (userland, l'espace mémoire utilisé par les programmes classiques) avec les risques (massifs) que cela implique question sécurité. La méthode décrite sur le blog tente d'exploiter les mécanismes d'exécution spéculative intégrés dans les CPU modernes.

Pour rappel, les processeurs modernes, depuis le Pentium Pro, sont de type OOO (Out Of Order), non seulement les instructions des programmes ne sont plus exécutées les unes derrière les autres exactement dans l'ordre dans lequel elles existent dans les programmes (certaines instructions sont anticipées, l'exemple typique est le cas des chargement en mémoire, dont la latence est coûteuse), mais elles peuvent être exécutées en parallèle par différentes unités d'exécution.

Le vecteur proposé s'attaque à ce mécanisme en tentant d'exploiter le moment entre lequel une instruction non autorisée (une lecture d'une adresse mémoire non autorisée) est exécuté et celui où il génère une erreur (une interruption). L'auteur du blog indique ne pas avoir réussi à lire la mémoire protégée via sa méthode, mais note que le chargement mémoire interdit est bel et bien effectué par le CPU même s'il ne copie jamais l'information dans le registre. Il note que l'exécution spéculative continue (dans les unités d'exécutions internes) jusqu'à ce que l'interruption soit effective, ouvrant la voie vers de multiples attaques potentielles basées par exemple sur les [temps d'exécution des instructions](#) pour déterminer les adresses mémoires utilisées par le kernel, et potentiellement d'autres types d'attaques.

Connaître les adresses mémoires utilisées par le kernel, à partir d'un programme userland, est quelque chose que les systèmes d'exploitation tentent de rendre impossible par différentes techniques depuis des années, une des méthodes les plus efficace étant l'ASLR ([Address Space Layout Randomization](#)) pour rendre aléatoires les adresses mémoires utilisées par les applications (et le kernel).

Depuis fin octobre, [un patch est en développement pour Linux](#) pour tenter d'imposer de nouvelles restrictions et mieux protéger les espaces mémoires du noyau. Ce patch a été significativement réécrit et porte le nom de KPTI (Kernel Page-Table Isolation) qui comme son nom l'indique tente de séparer les tables qui pointent vers les pages mémoires utilisées par le noyau de toutes les autres.





Ce patch qui est encore en cours de développement mais il est significatif par son coût important sur les performances pour certains types d'applications. En pratique, ce sont les applications qui effectuent beaucoup d'appels aux instructions systèmes (syscall) qui sont les plus touchées.

Les premiers benchmarks réalisés sur ces nouveaux patches par nos [confrères de Phoronix](#) pointent des chutes de performances très significatives dans les benchmarks théoriques sur les I/O disques. Pour les tests pratiques, les plus gros perdants semblent être (assez logiquement) les logiciels de base de données avec des impacts variables jusqu'ici allant de 6% à 25% pour Postgres. Redis, dans la même veine, semble également notablement impacté.

### Contenus relatifs

09/05: AMD Ryzen 7 2700, Ryzen 5 2600 et I...	[+]
04/05: Un Coffee Lake 8 coeurs en préparat...	[+]
27/04: Le 10nm d'Intel (encore) retardé, I...	[+]
26/04: Jim Keller rejoint... Intel !	[+]
19/04: 2008-2018 : tests de 62 processeurs...	[+]
10/04: LGA4189 pour les Xeon Ice Lake !	[+]
05/04: Pas de MAJ Microcode pour les Gultf...	[+]
03/04: Intel lance la 2ème vague de sa 8èm...	[+]
15/03: Microcode final pour Spectre chez I...	[+]
19/02: Intel présente un prototype de (min...	[+]

### Comparateur de prix

	AMD Ryzen 7 2700X Wraith ... Processeurs	» 306.50 €
	Intel Xeon E3-1270V5 (3.6... Processeurs	» 364.96 €
	Intel Xeon E3-1275V6 (3.8... Processeurs	» 401.99 €
	Intel Core i7-8700K (3.7 ... Processeurs	» 370.00 €

### Sondage

#### Envisagez-vous de passer à RX Vega ?

Oui, en version RX Vega 64 - 10.39%	<div style="width: 10.39%;"></div>
Oui, en version RX Vega 56 - 8.23%	<div style="width: 8.23%;"></div>
Oui, mais j'attendrais les customs - 12.3%	<div style="width: 12.3%;"></div>
Non, j'ai déjà un GPU équivalent ou supérieur - 24.44%	<div style="width: 24.44%;"></div>
Non, mon budget GPU est inférieur à 399\$ - 16.87%	<div style="width: 16.87%;"></div>
Non, je n'ai pas besoin d'un GPU si performant - 11.06%	<div style="width: 11.06%;"></div>
Non, j'attends la prochaine génération - 16.71%	<div style="width: 16.71%;"></div>

### Top articles

### Shop HardWare.fr

Achat processeur pas cher
Achat processeur Intel pas cher

**Alex Ionescu**

@aionescu



Windows 17035 Kernel ASLR/VA Isolation In Practice (like Linux KAISER). First screenshot shows how NtCreateFile is not mapped in the kernel region of the user CR3. Second screenshot shows how a 'shadow' kernel trap handler, is (has to be).

```

'oc ImageFileName Pcb.DirectoryTableBase P<c ImageFileName Pcb.DirectoryTableBase f
leBase      : 0x66000000          eBase      : 0x66000000
yTableBase  : 0x00000004 61600000 TableBase   : 0x00000004 61600000
             : [15] "windbg.exe"          : [15] "windbg.exe"

shadow
i3738715776 = fffff800 8c53dd80          736862064 = fffff800 8c702690
f8008c53dd80          8008c702690
c53dd80, pagedir 0000000066000000      702690, pagedir 0000000066000000
06600f80          6600f80
03f08010          f08010
0f09310           09318
ped phys 000000460d3dd80              ed phys 000000460b02690
c53dd80 translates to physical address 46f00000 fffff8008c53dd80          702690 translates to physical address 46f00000 fffff8008c702690
c53dd80, pagedir 0000000461600000      702690, pagedir 0000000461600000
061600f80          1600f80
03e61010          e61010
0c60310           60318
02679e8
00000460d3dd80
c53dd80 translates to physical address 46f02690 translation fails, error 0xD00001

```

1:30 PM · Nov 14, 2017

**169** Retweets **302** Likes*Microsoft a été réactif en appliquant également un patch de ce type*

Pour une utilisation non serveur, tout semble pointer vers un impact nul ou infinitésimal, pour preuve, Microsoft semble avoir également appliqué le même type de patch dès novembre dans Windows 10 [☞](#). Au delà de benchmarks synthétiques, l'impact devrait être réduit, on peut le voir dans les benches de Phoronix ou FFMpeg, x264 et la compilation d'un noyau Linux ne sont pas impactés.

Côté serveur l'impact est donc plus large, et semble toucher assez massivement les infrastructures Cloud où la virtualisation est largement utilisée et cette dernière particulièrement utilisatrice de *syscalls* pour isoler les espaces mémoires des machines virtuelles.

L'impact pratique final restera à mesurer, ce patch sera déployé dans la prochaine version du kernel (4.16) d'ici quelques semaines. Et il sera important de suivre quels CPU seront concernés en pratique. Car si le [patch tel qu'appliqué actuellement sur le git ☞](#) est appliqué de manière indiscriminée à tous les processeurs x86 (les architectures ARM/RISC ne semblent pas touchées), [AMD a demandé à ce que ce patch ne soit pas appliqué sur leurs processeurs ☞](#), indiquant que les microarchitectures du constructeur n'autorisent pas les références mémoires et les exécutions spéculatives qui semblent pointées par le premier blog plus haut dans cet article.

Il sera intéressant de suivre si, oui ou non, ce patch d'AMD sera accepté dans les prochaines semaines. On suppose qu'AMD dispose de détails encore sous embargo pour clamer ne pas être touché même s'il faut probablement être assez prudent sur la question tant que les détails ne sont pas dévoilés publiquement.

← Bonne année 2018 !

Meltdown et Spectre : un point sur les d... ▶

Vos réactions



annales  
le 03-01-2018 à  
13:51:32

Si je comprends bien le patch est software mais le bug est soft ou hardware?



Zerist  
le 03-01-2018 à  
13:58:43

Merci C\_Wiz pour cet article, c'est très clair 🧐



h3bus  
le 03-01-2018 à  
13:59:12

Le bug est hardware. Cela dit, il semble que ce n'est pas vraiment un bug mais une vulnérabilité non anticipée.



helionn  
le 03-01-2018 à  
14:05:42

Si AMD passe au travers leur cpu vont prendre un boost de compétitivité intéressant sur serveur.



Sympa comme nouvelle de début d'année pour AMD mais beaucoup moins sympa pour les gens qui gèrent un parc de bécane Intel...

Yog Sothoth  
le 03-01-2018 à  
14:08:51

Article qui vient tôt et avec de la substance. Bravo. 🧐



kurosu  
le 03-01-2018 à  
14:09:11

[EDIT commentaire incorrect] Pour le coût du correctif, cf. le bug TLB chez AMD il y a quelques années.



Un mauvais point par contre pour la réutilisation directe du subscriber link de LWN, qui est certes reposté tel quel à travers tous les media. Mais sans en citer la source initiale (que je ne retrouve vraiment pas /o).

luckan  
le 03-01-2018 à  
14:10:09

merci pour cet article très intéressant. Je rejoins h3bus, je pense qu'il s'agit d'une vulnérabilité non anticipée plutôt qu'un bug



d750  
le 03-01-2018 à  
14:15:34

On sait si un patch est prévu pour Windows7, et pour quand?



crypto  
le 03-01-2018 à  
14:16:43

Merci pour ce point sur la situation 🧐



C\_Wiz  
Equipe HardWare.fr  
le 03-01-2018 à  
14:22:20

Citation :  
Un mauvais point par contre pour la réutilisation directe du subscriber link de LWN, qui est certes reposté tel quel à travers tous les media. Mais sans en citer la source initiale (que je ne retrouve vraiment pas /o).



Je suis probablement tombé sur ce lien dans les commentaires de Hacker News. Je vais le retirer du coup thx.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 ▶

Ajouter un commentaire

OK

[\[+\] Afficher le sujet dans le forum](#)