Training Solo : Spectre V2 revient hanter des dizaines de CPU Intel et ARM

We came. We saw. We kicked its ass.

Des chercheurs ont découvert de multiples problèmes dans la manière dont les failles Spectre v2 avaient été gérées sur les processeurs Intel et ARM, constituant autant de nouvelles vulnérabilités. Ces dernières sont regroupées sous l'appellation Training Solo et nécessitent plusieurs correctifs. Intel fournit déjà un nouveau microcode.

Vincent Hermann , **Sébastien Gavois**

Le 13 mai à 12h00

6 min | Sécurité

On revient une fois encore sur la prédiction de branche et la possibilité pour des malwares d'entrainer spécifiquement cette dernière pour conduire les processus à laisser fuiter des informations. C'était la base des attaques Spectre et leurs variantes, dont la V2 dont il est question ici.

Pour circonscrire le problème, les constructeurs ont intégré des techniques d'isolation de domaines comme IBPB (Indirect Branch Predictor Barrier), ainsi qu'eIBRS (enhanced Indirect Branch Restriction Speculation) et BHI_NO (Branch History Injection) chez Intel.

Sur ces sujets, Oracle a publié récemment un long billet de blog. Ce n'est pas la première fois que Spectre revient d'outre-tombe, comme nous l'expliquions en novembre. En ce mois de mai 2025, elle

1

Hardware 07/11/2024 10h48

L'ombre de Spectre n'en finit plus de venir hanter les CPU

Problème, ces techniques d'isolation ne sont pas suffisantes. Selon les chercheurs de VUSec qui ont publié leurs travaux hier soir (après une période non-divulgation de plus d'un an), le constat est pire : même une isolation parfaite ne serait pas suffisante, car les défenses resteraient poreuses.

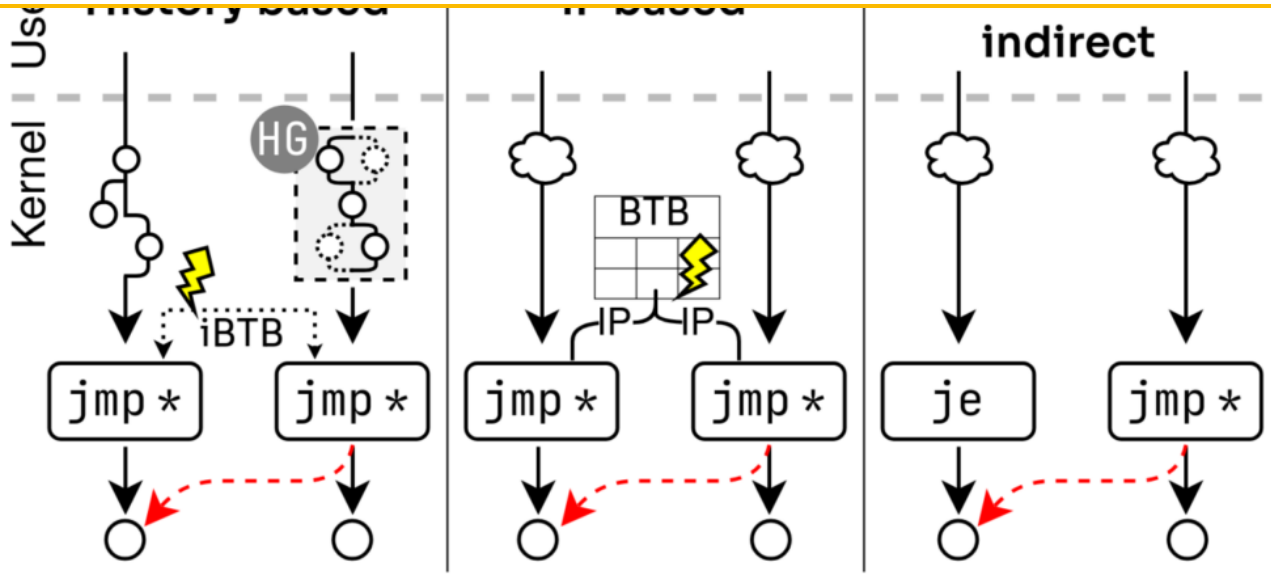
Les chercheurs disent avoir eu une idée : un auto-entrainement pourrait-il être réalisé dans un domaine privilégié (noyau ou hyperviseur par exemple) ? Non seulement la chose est possible, mais elle permet d'exploiter ensuite le mécanisme pour aboutir à des fuites de données, dans une nouvelle forme d'attaque par canal auxiliaire.

La vitesse de transmission des informations peut atteindre 17 ko/s, largement suffisante pour rendre l'attaque efficace. Une large gamme de processeurs Intel est concernée, certains de chez ARM aussi. AMD affirme être épargné.

Pas une, pas deux, mais trois variantes

Comme si le problème n'était pas assez sérieux, les chercheurs indiquent que leur attaque peut se décliner en trois variantes et que chacune a besoin d'un correctif spécifique. Il y a d'abord les attaques basées sur l'historique des instructions, permettant de contourner l'isolation du domaine en créant des historiques de branches et d'orienter ensuite la prédiction vers un module de divulgation. Intel a mis en ligne un article dédié.

Quand la prédiction basée sur l'historique est désactivée, il est possible de forcer quand même le prédicteur à revenir à des prédictions basées sur des adresses prévisibles. La technique ouvre la voie à deux branches indirectes pouvant s'entrainer l'une l'autre. Enfin, sur certains processeurs, les branches directes peuvent entrainer la prédiction de branche indirecte.



Tous les CPU touchés par Spectre-V2 le sont aussi pas Training Solo

Pour les chercheurs, leurs travaux montrent qu'il est possible de rompre les isolations mises en place. Cependant, il existe des problèmes dans l'implémentation matérielle des mécanismes de défense. « *Les problèmes matériels constatés par notre suite de tests rompent également la mise en œuvre de l'isolation, car les branches directes étaient supposées ne pas être utilisées pour l'entraînement des branches indirectes* », ajoutent les chercheurs. L'isolation de l'utilisateur et l'invité saute, tout comme celle de l'hyperviseur, rouvrant la voie aux « *attaques classiques de formation croisée Spectre-V2* ».

En somme, tous les processeurs affectés par Spectre-V2 le sont également par Training Solo. « *Même les systèmes pour lesquels toutes les mesures d'atténuation connues sont activées peuvent être vulnérables* » tant que les nouveaux correctifs ne sont pas appliqués, affirme VUsec.

Voici un résumé de VUcode sur les processeurs concernés par les différentes failles :

- **Attaques basées sur l'historique** : tous les processeurs Intel avec eIBRS (y compris donc Lion Cove) et certains processeurs ARM.
- **Indirect Target Selection (ITS)** (CVE-2024-28956) : concerne les processeurs Intel Core de 9e à 11e générations et Xeon de 2e et 3e générations.
- **Lion Cove BPU** (CVE-2025-24495) : Uniquement les processeurs Lunar Lake et Arrow Lake.

Intel	9900K	Coffee Lake R	Coffee Lake	○	◐	●	–	–	–	–	✗	✗
	10700K	Comet Lake	Comet Lake	◒	◐	○	●	–	–	–	✓	✓
	11700	Rocket Lake	Cypress Cove†	◒	◐	○	●	–	–	–	✓	✓
	11800H	Tiger Lake	Willow Cove†	◒	◐	○	●	–	–	–	✓	✓
	14900K	Raptor Lake	Raptor Cove‡	–	◐	○	●	●	○	–	✓	✗
			Gracemont§	–	◐	○	●	●	○	–	✗	✗
	155H	Meteor Lake	Redwood Cove‡	–	◐	○	●	●	○	–	✓	✗
			Crestmont§	–	◐	○	●	●	○	–	✓	✗
	258V	Lunar Lake	Lion Cove	–	◐	○	●	○	○	●	✓	◔
			Skymont§	–	◐	○	●	○	○	●	✓	◔
AMD	7950X	Raphael	Zen 4	–	◐	○	●	–	–	–	✗	✗
	9950X	Granite Ridge	Zen 5	–	◐	○	●	–	–	–	✗	✗

● Enabled by default, ◐ Enabled for cross-context, ◒ Enabled for cross-privileged, ○ Available, – Not available, ◔ Prediction after x privileged-branches, † Based on Sunny Cove, ‡ Based on Golden Cove, § Atom μarch.

Correctifs chez Intel, directives chez ARM, AMD épargné ?

Une série de correctifs et de mises à jour du microcode des processeurs est déjà prête, expliquant l'accord de non-divulgation des chercheurs. Chez Intel, de nouvelles versions de microcodes ont été publiées pour un très grand nombre de processeurs, des Core Ultra 200 aux Core de 8e génération (Coffee Lake), ainsi qu'une ribambelle de Xeon. Certaines attaques peuvent, en effet, fonctionner jusque sur les cœurs Lion Cove, utilisés dans les dernières générations de processeurs (Lunar Lake et Arrow Lake).

Dans leur publication scientifique (accompagné d'un dépôt GitHub), les chercheurs affirment avoir prévenu les fabricants et éditeurs dès mars 2024, soit il y a plus d'un an. Intel a confirmé et publié deux CVE (CVE2024-28956 et CVE-2025-24495) ainsi que deux avis (Intel-SA-01153 pour ITS et Intel-SA-01322 pour le problème Lion Cove).

De son côté, AMD « *a confirmé que ses mesures d'atténuation existantes étaient suffisantes* », indique VUsec. Enfin, ARM « *a confirmé que les analyses de l'attaque basée sur l'historique s'appliquent également* » à certains processeurs. ARM « *a publié une mise à jour de sécurité sur son site web dédié aux développeurs* », qui ne semble pas publiquement accessible.

Il faut aussi mettre à jour son système d'exploitation

Il faut mettre à jour le processeur, mais aussi le système d'exploitation. Sur Linux, comme souligné par Phoronix, plusieurs correctifs sont prêts et seront publiés prochainement. Chez Microsoft, il n'y a pas encore d'annonce particulière. Cependant, les mises à jour mensuelles de sécurité seront disponibles ce soir et pourraient intégrer des correctifs liés à Training Solo.

Vincent Hermann , Sébastien Gavois

Le 13 mai à 12h00

Commentaires (1)

Quelque chose à dire ?

Neliger

Aujourd'hui à 12h14

La blasitude des failles CPU 🔥

1