Hewlett Packard Enterprise

Rapport

HPE Customer Guidance Pack : Pallier la vulnérabilité des microprocesseurs dans l'ensemble du secteur

Dernière mise à jour : 21 mars 2018

Contents

Toutes les mémoires ROM de systèmes de serveurs HPE Gen10, Gen9, Gen8, G7, et G6, basés sur Intel, désormais disponibles

À compter du 19 mars 2018, les nouvelles mémoires ROM de systèmes de tous les serveurs HPE Gen10, Gen9, Gen8, G7 et G6, basés sur Intel®, ont été publiées sur le site Web d'assistance HPE. HPE conseille à ses clients de mettre à jour leurs serveurs HPE avec les nouvelles mémoires ROM de système afin de réduire le risque lié aux vulnérabilités de l'analyse par canal auxiliaire.

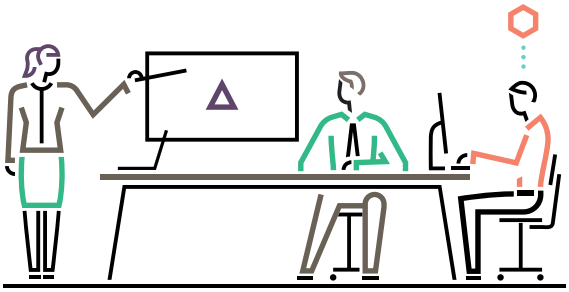
De plus, la mémoire ROM de système destinée au serveur HPE ProLiant DL385 Gen10, basé sur AMD, qui inclut un support pour la réduction des vulnérabilités de l'analyse par canal auxiliaire est disponible sur le site Web d'assistance HPE depuis le début du mois de janvier 2018.

Alerte Intel : 22 janvier 2018

Nous avons attiré l'attention de nos clients sur la déclaration d'Intel publiée le 22 janvier 2018 signalant des problèmes associés au correctif de microcode Intel conçu pour traiter la vulnérabilité liée à l'analyse par canal auxiliaire, susceptible de provoquer un « comportement imprévu du système ». Si les clients HPE ont téléchargé une mémoire ROM de système dédiée à cette vulnérabilité, pour un serveur basé sur Intel entre le 5 janvier et le 21 janvier 2018, HPE recommande de télécharger les nouvelles mémoires ROM de système, désormais disponibles, et de mettre à jour les serveurs en conséquence.

Consultez les pages Intel Security Exploit Newsroom et HPE Customer Advisory pour en savoir plus.

Contexte



Une vulnérabilité qui touche toutes les architectures de microprocesseur modernes a été récemment découverte. Selon une nouvelle étude sur la sécurité, il existe des méthodes d'analyses logicielles qui, lorsqu'elles sont utilisées à des fins malveillantes, ont la capacité de collecter de manière incorrecte des données sensibles provenant des appareils de calcul, qui fonctionnent par ailleurs comme prévu. Souvent appelée la méthode d'analyse par canal auxiliaire ou encore Spectre et Meltdown, cette vulnérabilité affecte les architectures de processeurs de plusieurs fournisseurs de CPU, dont Intel, AMD et Arm®.

Pour traiter cette vulnérabilité, les fournisseurs de matériel et de logiciels de l'ensemble du secteur, y compris HPE, ont travaillé en étroite collaboration à la publication de résolutions appropriées. Ce document HPE fournit aux clients un ensemble de conseils destinés à simplifier la démarche d'atténuation du risque lié à cette vulnérabilité.
Il comporte des procédures détaillées et une liste de liens importants vers les mises à jour de systèmes d'exploitation et de microcodes les plus usités dans les générations actuelles des serveurs HPE. HPE recommande également à ses clients d'examiner les déclarations publiées par les fournisseurs de microprocesseurs : Intel, AMD et ARM.

Conseils aux clients HPE

La sécurité des produits HPE est notre principale priorité et nous continuons de travailler de manière proactive avec les fournisseurs de systèmes d'exploitation et de microprocesseurs afin de développer des mises à jour des logiciels et de microprogrammes permettant de pallier la vulnérabilité des microprocesseurs.

Il est important de noter que la méthode d'analyse par canal auxiliaire nécessite qu'un programme malveillant s'exécute localement sur un système. Cette vulnérabilité spécifique n'active pas directement une modification, une suppression, une destruction ou un chiffrement des données, mais des données sont susceptibles d'être extraites des systèmes de l'ordinateur. Par conséquent, il est essentiel de conserver une bonne démarche de sécurité, qui implique des logiciels et des microprogrammes toujours à jour. Le respect des meilleures pratiques en matière de sécurité et le déploiement des serveurs HPE Gen10 dotés de la technologie sécurisée de racine de confiance au silicium, peuvent contribuer à protéger votre entreprise des attaques malveillantes.

Mesures d'atténuation des risques recommandées

HPE recommande à tous les clients de suivre les étapes suivantes pour les produits serveurs et de stockage afin de définir leur plan d'évaluation et d'atténuation des risques.

Produits serveurs :

* En appliquant les mises à jour de système d'exploitation, vous assurez une protection contre certaines variantes de vulnérabilité, même s'il n'existe pas de mises à jour de ROM de système disponibles.

** Si les clients HPE ont téléchargé une mémoire ROM de système dédiée à cette vulnérabilité, pour un serveur basé sur Intel entre le 5 janvier et le 21 janvier 2018, HPE recommande de télécharger les nouvelles mémoires ROM de système, désormais disponibles, et de mettre à jour les serveurs en conséquence.

Produits de stockage :

Foire aux questions (FAQ)

1. La vulnérabilité du microprocesseur touche-t-elle tous les fournisseurs de cette technologie ou bien uniquement HPE ?

La vulnérabilité du microprocesseur touche tous les fournisseurs de technologies qui utilisent des microprocesseurs modernes et n'est pas spécifique à HPE. Tous les produits et solutions impactés par cette vulnérabilité requièrent des mises à jour appropriées du système d'exploitation et de mémoire ROM. Intel a déclaré que les processeurs Itanium® n'étaient pas impactés par la vulnérabilité liée à l'analyse par canal auxiliaire.

2. Quels produits et solutions HPE sont impactés ?

Tous les produits HPE qui intègrent les microprocesseurs touchés sont potentiellement vulnérables. Pour déterminer si vos produits et solutions HPE sont concernés, veuillez consulter la page Web HPE consacrée à la vulnérabilité HPE. HPE mettra à jour la liste de tous les systèmes si nécessaire.

3. La vulnérabilité du microprocesseur est-elle due à une attaque active ou à un piratage ?

Non, il n'y a pas eu d'attaques connues. Cette vulnérabilité des microprocesseurs est due à un défaut de conception, qui peut permettre à quelqu'un de récupérer des données, si l'analyse est effectuée via la méthode d'analyse par canal auxiliaire. En appliquant les mises à jour appropriées du système d'exploitation et du microprocesseur sur vos systèmes HPE, cela réduit le risque associé à cette vulnérabilité.

4. Quelle est l'ampleur de cette faille de sécurité ?

Une nouvelle étude sur la sécurité a permis d'identifier des méthodes d'analyses logicielles qui, lorsqu'elles sont utilisées à des fins malveillantes, ont la capacité de collecter de manière incorrecte des données sensibles provenant des appareils de calcul, qui fonctionnent par ailleurs comme prévu. Pour en savoir plus, consultez les cas courants suivants d'exposition à ces failles : CVE-2017-5715, CVE-2017-5753, CVE-2017-5754.

5. En quoi consiste la résolution ?

Pour venir à bout de cette vulnérabilité, il est nécessaire de procéder à une mise à jour et du système d'exploitation, disponible auprès du fournisseur du système d'exploitation, et de la mémoire ROM du système, fournie par HPE. En fonction du système HPE que vous exécutez, vous pouvez retrouver des instructions sur les actions appropriées à mettre en œuvre en consultant la page Web HPE consacrée à la vulnérabilité.

Si vous êtes client HPE Pointnext et si vous croyez que vous exécutez un système impacté, contactez l'équipe d'assistance.

Si vous êtes un client de solutions HPE Storage, vous pouvez retrouver des instructions sur les actions appropriées à mettre en œuvre sur la page Web HPE consacrée à la vulnérabilité. Les procédures de correction des produits HPE Storage peuvent différer de celles des produits pour serveurs HPE. Veuillez consulter la page Web HPE consacrée à la vulnérabilité pour plus de détails sur le stockage. Pour les produits logiciels tels que StoreVirtual VSA, StoreOnce VSA, RMC, et d'autres noms de logiciels exécutés sur des serveurs basés sur x86, il vous est conseillé de consulter les déclarations émises par le fournisseur de votre serveur x86.

6. Pour télécharger et installer les mises à jour de ROM du système HPE, est-il obligatoire de détenir un contrat ou une garantie en cours de validité ?

Non. Nous levons l'obligation de contrôle des droits pour les mises à jour de ROM de système HPE pour les produits et solutions impactés par cette vulnérabilité, le cas échéant.

7. Quels systèmes d'exploitation sont impactés ?

Windows®, Linux® et VMWare® sont impactés. Les fournisseurs des systèmes d'exploitation mettent à disposition de leurs clients des mises à jour correctives des systèmes d'exploitation. À l'appui de la déclaration actuelle émise par Intel, Itanium n'est pas touché, ce qui signifie que les systèmes d'exploitation HP-UX, OpenVMS et NonStop sur les séries NonStop J et H ne sont pas touchés. S'exécutant sur des processeurs x86, les systèmes d'exploitation NonStop sur les séries NonStop L sont touchés. En outre, comme les modules CLIM et NSC dans les systèmes NonStop s'exécutent sur des processeurs x86, et les systèmes d'exploitation Linux et Windows sur ces composants de systèmes NonStop sont touchés. Pour en savoir plus, HPE recommande de contacter les fournisseurs des systèmes d'exploitation : Microsoft®, VMware, SUSE, and Red Hat®.

8. Quels microprocesseurs sont impactés ?

La plupart des microprocesseurs dotés d'architectures modernes peuvent être impactés par la méthode d'analyse des canaux auxiliaires. Intel et AMD ont contacté HPE de manière proactive et ont collaboré activement avec HPE pour apporter des solutions. Intel a déclaré que les processeurs Itanium n'étaient pas impactés par la vulnérabilité liée à l'analyse par canal auxiliaire. Concernant tous les autres fournisseurs de microprocesseurs, contactez le fournisseur du processeur pour en savoir plus.

9. Est-ce que d'autres fabricants de matériel sont touchés ?

Tous les fabricants de matériel ainsi que les prestataires de services de clouds publics qui utilisent des architectures de microprocesseurs modernes sont susceptibles d'être impactés. Les téléphones mobiles et les ordinateurs clients peuvent également être impactés ; adressez-vous aux fournisseurs de ces produits pour en savoir plus.

10. Une fois le correctif appliqué à mes systèmes, dois-je m'attendre à une incidence sur les performances ?

Dans la plupart des cas, nous prévoyons une incidence réduite à un niveau minimal sur les performances mais son amplitude peut varier en fonction du système d'exploitation et de la charge de travail. HPE et ses partenaires fournisseurs de systèmes d'exploitation et de microprocesseurs continueront de surveiller et de définir l'impact au niveau des performances au fil du temps et fourniront des conseils supplémentaires au fur et à mesure de la mise à disposition de données.

11. Que signifie cette vulnérabilité des microprocesseurs pour les serveurs HPE ProLiant et HPE Synergy Gen10, les serveurs du secteur les plus sécurisés au monde ?[1]

La vulnérabilité des microprocesseurs représente une faille dans les microprocesseurs modernes : néanmoins, il n'existe pas d'attaques connues liées à cette vulnérabilité. Les serveurs HPE Gen10 disposent de la seule véritable technologie de racine de confiance au silicium. Ce silicium HPE conçu sur mesure garantit une protection inégalée contre les attaques du microprogramme. Malgré nos fonctions de sécurité renforcées, en ce qui concerne cette vulnérabilité spécifique, les clients doivent continuer à appliquer toutes les mises à jour recommandées et respecter les meilleures pratiques en matière de sécurité.

12. Que signifie cette vulnérabilité des microprocesseurs pour les clients qui envisagent d'acheter des produits HPE ?

Vous pouvez être assuré que les solutions de calcul HPE sont à la pointe de la technologie en matière de sécurité et de qualité. La découverte de cette vulnérabilité des microprocesseurs dans l'ensemble du secteur, ne devrait pas impacter votre décision d'acheter des solutions HPE. HPE poursuivra sa collaboration avec Intel, AMD et ARM pour garantir que les résolutions requises pour les microprocesseurs utilisés dans nos produits, restent la principale priorité. En outre, lorsque les mises à jour des microprocesseurs sont appliquées et combinées avec la technologie HPE de racine de confiance au silicium, disponible uniquement dans les serveurs HPE Gen10, nos clients peuvent être assurés que leur plate-forme de calcul répond aux normes de sécurité les plus strictes du secteur.

13. Est-ce que HPE fournira des mises à jour supplémentaires concernant cette vulnérabilité ?

Oui, HPE continuera de publier des mises à jour au fur et à mesure de la mise à disposition d'informations et de détails supplémentaires. Vous pouvez vous reporter à la page Web HPE consacrée à la vulnérabilité à l'adresse HPE consacrée à la vulnérabilité HPE..

14. Récemment, HPE avait mis à disposition des mises à jour de ROM de système pour les produits pour serveurs HPE ProLiant, HPE Synergy, HPE Superdome Flex, et HPE Superdome X. Pourquoi ne puis-je pas les trouver actuellement ?

Depuis le 19 mars 2018, des mises à jour sont disponibles pour tous les serveurs HPE Gen10, Gen9, Gen8, G7, et G6, basés sur Intel, et pour le serveur HPE ProLiant DL385 Gen10, basé sur AMD.

Le 22 janvier 2018, Intel a publié une déclaration relative aux problèmes concernant le correctif de microcode Intel, conçu pour faire face à la vulnérabilité engendrée par l'analyse par canal auxiliaire. A ce moment-là, Intel avait recommandé que les clients arrêtent de déployer des ROM de système comprenant ce correctif de microcode et de revenir à leur version précédente de ROM de système afin d'éviter tout comportement inattendu de leur système. Par conséquent, HPE a retiré du site d'assistance HPE, les mises à jour de ROM de système existantes destinées aux produits pour serveurs HPE ProLiant, HPE Synergy, HPE Superdome Flex, et HPE Superdome X.
Depuis lors, Intel a procédé à des révisions sur le microcode ; des mémoires ROM de système sont désormais disponibles pour tous les serveurs HPE Gen10, Gen9, Gen8, G7, et G6, basés sur Intel. Des révisions actualisées des ROM de système pour d'autres plates-formes seront mises à disposition par HPE dès qu'Intel aura fourni des microcodes mis à jour.

[1] Sur la base d'un test de pénétration lié à la cybersécurité réalisé par une entreprise externe à partir d'une gamme de produits serveur de plusieurs fabricants, mai 2017.

15. Quelles générations de serveurs HPE recevront les mises à jour de ROM de système qui contiennent les microcodes permettant une atténuation de la vulnérabilité lié à l'Analyse par canal auxiliaire ?

HPE s'est engagé dans un processus d'étroite collaboration avec les fournisseurs de microprocesseurs pour fournir des mises à jour de ROM de système destinées aux serveurs HPE Gen10, Gen9, Gen8, G7, et de générations plus anciennes, au fur et à mesure que les fournisseurs de processeurs fourniront des mises à jour de microcodes.

À toutes fins utiles, adressez-vous directement à votre représentant commercial HPE ou à votre partenaire autorisé afin d'obtenir des informations supplémentaires et une assistance.

Inscrivez-vous pour les mises à jour

a00039576FRE, mars 2018, Rév. 2