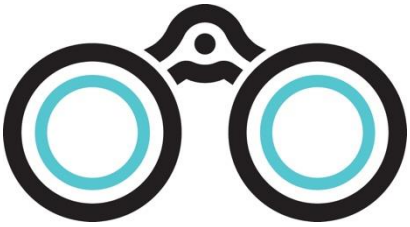
Hewlett Packard Enterprise

Guía para clientes HPE:
Mitigación de la vulnerabilidad de microprocesador en toda la industria

5 January 2018

Antecedentes.



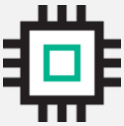
Recientemente, se identificó una vulnerabilidad en toda la industria que involucra arquitecturas modernas de microprocesadores. Con base en una nueva investigación de seguridad, existen métodos de análisis de software que, cuando se utilizan con fines maliciosos, tienen el potencial de recopilar datos confidenciales de manera inadecuada de dispositivos informáticos que funcionan según lo diseñado. A menudo se lo conoce como “the Side-Channel Analysis Method, or Spectre and Meltdown” esta vulnerabilidad afecta las arquitecturas de microprocesadores de múltiples proveedores de CPU, incluidos Intel, AMD y ARM.

Para abordar esta vulnerabilidad, los proveedores de hardware y software de toda la industria, incluido HPE, han estado trabajando juntos para publicar las resoluciones adecuadas. Este documento de HPE es un paquete de orientación para clientes diseñado para simplificar la tarea de mitigar el riesgo de esta vulnerabilidad. Incluye instrucciones paso a paso y una compilación de enlaces importantes al sistema operativo (SO) más común y las actualizaciones de micro código utilizadas con las generaciones actuales del servidor HPE. HPE también recomienda que nuestros clientes revisen las declaraciones publicadas por los proveedores de microprocesadores: **Intel, AMD, and ARM.**

HPE Guía de orientación

La seguridad de los productos HPE es nuestra máxima prioridad y seguimos trabajando proactivamente con los proveedores de SO y microprocesadores para desarrollar actualizaciones de software y firmware para mitigar la vulnerabilidad del microprocesador.

HPE recomienda a todos los clientes que sigan los pasos a continuación para determinar su riesgo y plan de mitigación.

1	2	3	4
			
Determine si tiene un sistema que se ve afectado por esta vulnerabilidad. HPE está manteniendo un lista de productos afectados en el HPE vulnerability website.	Si su sistema se ve afectado, descargue e instale la actualización del sistema operativo proporcionada por el proveedor del sistema operativo. Según el sistema que esté ejecutando, puede encontrar instrucciones sobre las acciones apropiadas para tomar en el HPE Security Bulletin.	Actualice la ROM del sistema a una revisión que contenga un microcódigo actualizado de HPE. Dependiendo del sistema que esté ejecutando, puede encontrar instrucciones sobre las acciones apropiadas para tomar en el HPE Security Bulletin.	Reinicie el sistema afectado según sea necesario, garantizando las nuevas actualizaciones están completamente implementadas.

Un aspecto importante de the Side-Channel Analysis Method es que requiere malware para ejecutarse localmente en un sistema. Esta vulnerabilidad en particular no habilita directamente la alteración, eliminación, destrucción o encriptación de datos, pero es posible que los datos se extraigan de los sistemas informáticos. **Por lo tanto, es importante practicar una buena higiene de seguridad, incluyendo mantener siempre actualizados el software y el firmware. Seguir las mejores prácticas de seguridad y desplegar servidores HPE Gen10 con tecnología segura Silicon Root of Trust que puede ayudarlo a proteger su empresa contra ataques maliciosos.**

Tenga en cuenta que la ROM del sistema está disponible para los sistemas actuales HPE Gen9 y Gen10. Publicaremos actualizaciones para sistemas HPE Gen8 y anteriores en el futuro cercano.

Preguntas frecuentes

1. **¿La vulnerabilidad del microprocesador afecta a todos los proveedores de tecnología o esto es exclusivo de HPE.?**

   La vulnerabilidad del microprocesador no es exclusiva de HPE. La vulnerabilidad existe en toda la industria Todos los productos y soluciones que usan microprocesadores de un moderno la arquitectura se ve potencialmente afectada si una resolución no se ha implementado

2. **¿Qué productos y soluciones de HPE se ven afectados?**

   Cualquier producto HPE que incluya microprocesadores afectados es potencialmente vulnerable. Los productos y soluciones HPE que pueden verse afectados se enumeran en el HPE vulnerability website. HPE actualizará la lista según sea necesario

3. **¿La vulnerabilidad del microprocesador se debe a un ataque o violación activa?**
   No, no hubo un ataque real. Esta vulnerabilidad de microprocesador se debe a una falla de diseño que, cuando se analiza a través the side-channel methodology, puede permitir a alguien deducir datos. Cuando se aplican las correcciones de microprocesador y se combinan con la única tecnología genuina Silicon Root of Trust technology, nuestros clientes pueden estar seguros de que las soluciones de HPE están diseñadas para un ataque.
4. **¿Cuál es la magnitud de la vulnerabilidad?**
   La nueva investigación de seguridad describe métodos de análisis de software que, cuando se utilizan con fines maliciosos, tienen el potencial de recopilar datos confidenciales de manera inadecuada de dispositivos informáticos que funcionan según lo diseñado. Para obtener más información, consulte las siguientes exposiciones de vulnerabilidad comunes: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754.

5. **¿Cuál es la resolución?**
   La resolución de esta vulnerabilidad requiere una actualización del sistema operativo, proporcionada por el proveedor del sistema operativo, y una actualización de la ROM del sistema de HPE

   Dependiendo de los sistemas HPE que esté ejecutando, puede encontrar instrucciones sobre las acciones apropiadas para tomar en HPE Security Bulletin.

   Si usted es cliente de HPE Pointnext y cree que está ejecutando un sistema afectado, contacte a su representante de Soporte.

6. **¿Qué sistemas operativos se ven afectados?**

   Windows, Linux y VMWare se ven afectados. Los proveedores de sistemas operativos están proporcionando el parche del sistema operativo actualizaciones. Para obtener información adicional, HPE recomienda ponerse en contacto con los proveedores de sistemas operativos: Microsoft, VMware, SUSE y Red Hat**.**

7. **¿ Qué microprocesadores se ven afectados ¿**
   La mayoría de los microprocesadores con arquitecturas modernas pueden verse afectados por el método de análisis de canal lateral. Intel y AMD se han puesto en contacto de forma proactiva con HPE y están trabajando activamente con HPE para proporcionarle soluciones. Para todos los demás proveedores de microprocesadores, comuníquese con el proveedor del procesador para obtener más información**.**

8. **¿Se ven afectados otros fabricantes de hardware?**
   Todos los fabricantes de hardware, así como las nubes públicas que utilizan arquitecturas de microprocesadores modernos afectados, se ven potencialmente afectados. Los teléfonos móviles y las computadoras del cliente se ven afectados: consulte a los proveedores de esos productos para obtener más detalles.

9. **Después de parchear mis sistemas, ¿habrá un impacto asociado al rendimiento?**
   En la mayoría de los casos, el impacto en el rendimiento suele ser mínimo, pero varía según el sistema operativo y la carga de trabajo. HPE y nuestros socios de SO y microprocesadores caracterizarán el impacto en el rendimiento y proporcionarán más orientación a lo largo del tiempo.

10. **¿Qué significa esta vulnerabilidad de seguridad para los servidores HPE ProLiant y HPE Synergy Gen10, los servidores estándar de la industria más seguros del mundo?**
    HPE fabrica los servidores estándar de la industria más seguros del mundo. Esta vulnerabilidad particular afecta los sistemas operativos y los microprocesadores que utilizan nuestras soluciones. Sin embargo, los servidores estándar de la industria HPE tienen la única tecnología genuina **Silicon Root of Trust technology;** Anclando nuestro firmware en nuestro silicio de diseño personalizado HPE, proporciona una protección sin precedentes**.** A pesar de nuestras características de seguridad mejoradas, con respecto a esta vulnerabilidad en particular, los clientes aún deben aplicar todas las actualizaciones recomendadas y seguir las mejores prácticas de seguridad.

11. **¿Qué significa esta vulnerabilidad de microprocesador para los clientes que consideran comprar productos HPE?**
    Este es un problema en toda la industria y HPE está trabajando activamente en nombre de nuestros clientes para mitigar cualquier riesgo debido a esta vulnerabilidad. Los clientes pueden estar seguros de que HPE está haciendo todo lo posible y que esta vulnerabilidad de microprocesador no debe afectar las decisiones de compra de soluciones HPE.
12. **¿HPE proporcionará más actualizaciones con respecto a esta vulnerabilidad?**
    Sí, HPE continuará publicando actualizaciones a medida que haya más información y detalles disponibles. Puede consultar HPE Customer Bulletin.

Para obtener más información, contacte directamente con su representante de ventas de HPE o su socio autorizado para obtener más preguntas y ayuda.