A diferencia de las vulnerabilidades anteriores del canal lateral reveladas en las CPU de Intel, un grupo de investigadores descubrió una nueva falla que puede explotarse de forma remota por medio de la red sin requerir que un atacante tenga acceso físico o cualquier malware instalado en una computadora objetivo.

Nombrado como NetCAT, abreviación de Network Cache Attack, la nueva vulnerabilidad de canal lateral basada en la red, podría permitir a un atacante remoto detectar datos confidenciales, como la contraseña SSH de alguien.

Descubierta por un equipo de investigadores de seguridad de la Universidad de Vrije, Amsterdam, la vulnerabilidad registrada como CVE-2019-11184, reside en una función de optimización del rendimiento llamada DDIO de Intel, abreviatura de E/S directa de datos, que por diseño otorga dispositivos de red y otros periféricos acceden al caché de la CPU.

El DDIO viene habilitado de forma predeterminada en todos los procesadores Intel para servidores desde 2012, incluyendo las familias Intel Xeon E5, E7 y SP.

Según los investigadores, el ataque de NetCAT funciona similarmente a Throwhammer, al enviar únicamente paquetes de red especialmente diseñados a una computadora específica que tiene habilitada la función de acceso directo a memoria remota (RDMA).

RDMA permite a los atacantes espiar los periféricos remotos del lado del servidor, como las tarjetas de red, y observar la diferencia de tiempo entre un paquete de red que se sirve desde la caché del procesador remoto frente a un paquete servido desde la memoria.

Aquí la idea es realizar un análisis de sincronización de pulsación de tecla para recuperar palabras escritas por una víctima usando un algoritmo de aprendizaje automático contra la información de tiempo.

> *«En una sesión SSH interactiva, cada vez que se presiona una tecla, los paquetes de red se transmiten directamente. Como resultado, cada vez que una víctima*

> *escribe un carácter dentro de una sesión SSH encriptada en su consola, NetCAT puede perder el tiempo del evento al filtrar la hora de llegada del paquete de red correspondiente»,* explicó el equipo de VUSec.
>
> *«Ahora, los humanos tienen distintos patrones de escritura. Por ejemplo, escribir 'justo después de' es más rápido que escribir 'después de'. Como resultado, NetCAT puede operar análisis estáticos de los tiempos entre paquetes de llegadas en lo que se conoce como un ataque de tiempo de pulsación de tecla para filtrar lo que escribe en su sesión SSH privada».*

El equipo de VUSec también publicó un video, como se observa, que demuestra un método para espiar sesiones SSH en tiempo real con nada más que un servidor compartido.

NetCAT se convierte en la nueva vulnerabilidad de canal lateral unida a la lista de otras vulnerabilidades de canal lateral peligrosas descubiertas en el último año, incluyendo Meltdown, Spectre, TLBleed, Foreshadow, SWAPGS y PortSmash.

En su aviso, Intel reconoció el problema y recomendó a los usuarios que deshabiliten completamente DDIO o al menos RDMA para hacer que dichos ataques sean más difíciles, o sugirieron limitar el acceso directo a los servidores desde redes no confiables.

La compañía asignó a la vulnerabilidad de NetCAT una clasificación de gravedad «baja», describiéndola como un problema de divulgación de información parcial, y otorgó una recompensa al equipo de VUSec por la divulgación responsable de la información.