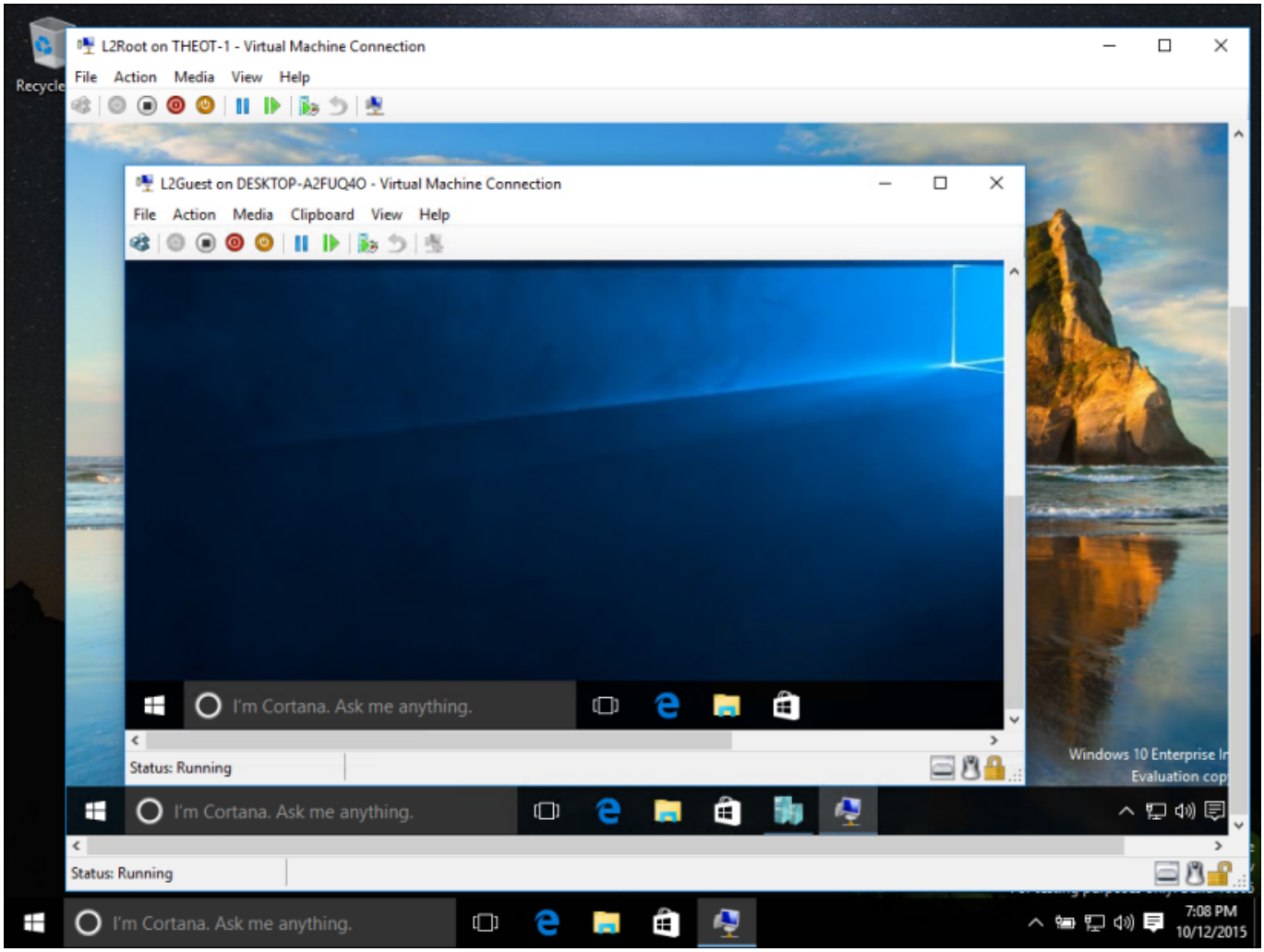
Ataques RDP inversos permiten el escape de invitado a host en Hyper-V

Autor: I. Stepanenko

Fecha: Monday 26th of August 2019 08:24:32 AM



A inicios de este año, los investigadores revelaron el secuestro del portapapeles y los problemas de recorrido en el cliente RDP incorporado de Windows que podría permitir que un servidor RDP malicioso comprometa a una computadora cliente, inversamente.

En el momento en que los investigadores informaron de forma responsable este problema de la ruta transversal a Microsoft, en octubre de 2018, la compañía reconoció el problema, también conocido como *"vulnerabilidad RDP envenenada",* pero decidió abordarlo.

Ahora, Microsoft al parecer parchó silenciosamente la vulnerabilidad CVE-2019-0887 el mes pasado, como parte de sus actualizaciones de martes de julio, luego de que Eyal Itkin, investigador de seguridad de CheckPoint, descubriera el mismo problema que afecta también

a la tecnología Hyper-V de Microsoft.

Hyper-V de Microsoft es una tecnología de virtualización que viene integrada con el sistema operativo Windows, lo que permite a los usuarios ejecutar múltiples sistemas operativos al mismo tiempo que las máquinas virtuales. El servicio en la nube Azure de Microsoft también utiliza Hyper-V para la virtualización del servidor.

Al igual que otras tecnologías de virtualización, Hyper-V también viene con una interfaz gráfica de usuario que permite a los usuarios administrar sus máquinas virtuales locales y remotas.

Según el reporte de los investigadores de CheckPoint, el modo de sesión mejorada en el Administrador de Hyper-V de Microsoft, detrás de escena, utiliza la misma implementación que los servicios de escritorio remoto de Windows para permitir que la máquina host se conecte a una máquina virtual invitada y comparta recursos sincronizados como datos del portapapeles.

> "Resulta que RDP se usa detrás de escena como el plano de control para Hyper-V. En lugar de volver a implementar el uso compartido de pantalla, teclado remoto y un portapapeles sincronizado, Microsoft decidió que todas las características ya están implementadas como parte de RDP, entonces, ¿Por qué no usarlo también en este caso?", dicen los investigadores.

RDP, que incluye el secuestro del portapapeles y las vulnerabilidades de recorrido de ruta que podrían conducir a un ataque de escape de VM de huésped a host, *"efectivamente permitiendo que uno salga de una máquina virtual y llegue a la máquina de alojamiento, prácticamente rompiendo la mitigación de seguridad más fuerte proporcionada por el entorno de virtualización".*

Como se demostró en el video, las fallas podrían permitir que una máquina invitada maliciosa o comprometida engañe al usuario host para que guarde sin saberlo un archivo malicioso en

su carpeta de inicio de Windows, que se ejecutará automáticamente cada vez que se inicie el sistema.

> "Un servidor RDP malicioso puede enviar un contenido de portapapeles de transferencia de archivos diseñado que provocará un recorrido transversal en la máquina del cliente", dicen los investigadores.

A diferencia de antes, en este caso Microsoft decidió parchear la vulnerabilidad inmediatamente luego de que los investigadores revelaran las implicaciones de Hyper-V de esta falla, ahora identificada como CVE-2019-0887.

> "El portapapeles compartido permite al usuario copiar un grupo de archivos de una computadora y pegar dichos archivos en otra computadora. Si el cliente no puede canonizar y desinfectar adecuadamente las rutas de archivos que recibe, podría ser vulnerable a un ataque transversal de ruta, permitir que un servidor RPD malicioso deje caer archivos arbitrarios en rutas arbitrarias en la máquina cliente", dijo Microsoft al explicar la vulnerabilidad.

> "Un atacante que explotara con éxito esta vulnerabilidad podría ejecutar código arbitrario en el sistema de la víctima. Luego, un atacante podría instalar programas, ver, cambiar, o eliminar datos, o crear nuevas cuentas con derechos de usuario completos", agregó.

Los investigadores probaron y confirmaron el parche para la vulnerabilidad Path-Transversal y recomendaron encarecidamente a todos los usuarios que instalen el parche de seguridad en un intento de proteger sus conexiones RDP y su entorno Hyper-V.

Ataques RDP inversos permiten el escape de invitado a host en Hyper-V

Autor: I. Stepanenko

Fecha: Monday 26th of August 2019 08:24:32 AM

Impactos: 69