Investigadores de seguridad cibernética de Check Point revelaron hoy los detalles de dos vulnerabilidades potencialmente peligrosas recientemente parcheadas en los servicios de Microsoft Azure, que de ser explotadas, podrían haber permitido a los hackers dirigirse a empresas que ejecutan sus aplicaciones web y móviles en Azure.

Azure App Service es un servicio integrado totalmente administrado que permite a los usuarios crear aplicaciones web y móviles para cualquier plataforma o dispositivo, e integrarlas fácilmente con soluciones SaaS, aplicaciones locales para automatizar procesos comerciales.

Según el informe de los investigadores, la primera vulnerabilidad identificada como CVE-2019-1234, es un problema de falsificación de solicitudes que afectó a Azure Stack, una solución de software de computación en la nube híbrida de Microsoft.

Si se explota, el problema habría permitido a hackers remotos acceder sin autorización a capturas de pantalla e información confidencial de cualquier máquina virtual que se ejecute en la infraestructura de Azure, no importa si se ejecutan en máquinas virtuales compartidas, dedicadas o aisladas.

Los investigadores aseguran que esta falla es explotable por medio de Microsoft Azure Stack Portal, una interfaz donde los usuarios pueden acceder a las nubes que crearon utilizando Azure Stack.

Al aprovechar una API asegurada, los investigadores encontraron una forma de obtener el nombre y la identificación de la máquina virtual, la información de hardware como núcleos, memoria total de las máquinas objetivo y luego utilizar dicha información con otra solicitud HTTP no autenticada para tomar capturas de pantalla como las siguientes.

Por otro lado, la segunda vulnerabilidad, identificada como CVE-2019-1372, es un error de ejecución remota de código que afectó al Servicio de Aplicaciones de Azure Stack, lo que habría permitido que un hacker tome el control completo de todo el servidor de Azure, y

como consecuencia, tomar el control de una empresa comercial.

Algo interesante es que un atacante puede explotar ambas vulnerabilidades creando una cuenta de usuario gratuita con Azure Cloud y ejecutando funciones maliciosas o enviando solicitudes HTTP no autenticadas al portal de usuario de Azure Stack.

Check Point publicó un aviso técnico detallado sobre la segunda vulnerabilidad, donde asegura que reside en la forma en que DWASSVC, un servicio responsable de administrar y ejecutar las aplicaciones de otros inquilinos y procesos de trabajo de IIS, que realmente ejecutan la aplicación del inquilino, se comunican entre sí para tareas definidas.

Dado que Azure Stack no puedo verificar la longitud de un búfer antes de copiarle memoria, un atacante podría haber explotado el problema al enviar un mensaje especialmente diseñado al servicio DWASSVC, permitiéndole ejecutar código malicioso en el servidor como la AUTORIDAD/SISTEMA NT de más alto privilegio.

> *«Entonces, ¿cómo puede un atacante enviar un mensaje a DWASSVC (DWASInterop.dll)? Por diseño, cuando ejecuta la función C# Azure, se ejecuta en el comando del trabajador (w3wp.exe). Esto le permite al atacante la posibilidad de enumerar los identificadores abiertos actualmente. De esa forma, puede encontrar el identificador de canalización con nombre ya abierto y enviar un mensaje especialmente diseñado»,* dijeron los investigadores.

Ronen Shustin, investigador de Check Point y quien descubrió ambas vulnerabilidades, informó responsablemente a Microsoft el año pasado, evitando que los hackers causen daños graves.

Después de solucionar los problemas a fines del año pasado, la compañía recompensó a Shustin con 40 mil dólares bajo su programa de recompensas por errores de Azure.