Posibles vulnerabilidades en la PowerShell Gallery podrían ser explotadas por agentes malintencionados para llevar a cabo ataques a la cadena de suministro contra los usuarios del registro.

> *«Estos problemas hacen que los ataques de suplantación de identidad sean inevitables en este registro, al mismo tiempo que dificultan en gran medida que los usuarios identifiquen al propietario legítimo de un paquete»,* informaron los investigadores de seguridad de Aqua, Mor Weinberger, Yakir Kadkoda e Ilay Goldman, en un informe.

Mantenido por Microsoft, PowerShell Gallery es un repositorio central para compartir y obtener código de PowerShell, que incluye módulos de PowerShell, scripts y recursos de Configuración de Estado Deseado (DSC). El registro cuenta con 11,829 paquetes únicos y un total de 244,615 paquetes.

Las cuestiones identificadas por la firma de seguridad en la nube están relacionadas con la política poco rigurosa del servicio en torno a los nombres de los paquetes, la carencia de protecciones contra ataques de suplantación de identidad, lo que resulta en que los atacantes puedan cargar módulos maliciosos de PowerShell que aparentan ser legítimos para los usuarios desprevenidos.

Una segunda vulnerabilidad se relaciona con la capacidad de un actor malicioso para falsificar los metadatos de un módulo, incluyendo los campos de Autor(es), Derechos de Autor y Descripción, con el fin de dar la apariencia de mayor legitimidad, engañando así a usuarios desprevenidos para que los instalen.

> *«La única manera para que los usuarios puedan determinar al autor/propietario real es abriendo la pestaña de 'Detalles del Paquete'»,* indicaron los investigadores.

> *«Sin embargo, esto solo los llevará al perfil del autor falso, ya que el atacante puede elegir libremente cualquier nombre al crear un usuario en la PowerShell Gallery. Por ende, identificar al autor verdadero de un módulo de PowerShell en la PowerShell Gallery se convierte en una tarea desafiante.»*

Además, también se descubrió una tercera vulnerabilidad que podría ser aprovechada por atacantes para enumerar todos los nombres y versiones de los paquetes, incluyendo aquellos que no están listados y que están destinados a permanecer ocultos a la vista pública.

Esto puede ser logrado mediante la utilización de la API de PowerShell *«https://www.powershellgallery.com/api/v2/Packages?$skip=number,»* permitiendo que un atacante obtenga acceso ilimitado a la completa base de datos de paquetes de PowerShell, incluyendo las versiones asociadas.

> *«Este acceso no controlado brinda a los actores maliciosos la capacidad de buscar información potencialmente sensible dentro de paquetes no listados. En consecuencia, cualquier paquete no listado que contenga datos confidenciales se vuelve altamente vulnerable a ser comprometido»,* explicaron los investigadores.

Aqua afirmó haber informado de estas debilidades a Microsoft en septiembre de 2022, después de lo cual se dice que el fabricante de Windows implementó soluciones reactivas a partir del 7 de marzo de 2023. Sin embargo, los problemas siguen siendo reproducibles.

> *«A medida que dependemos cada vez más de proyectos y registros de código abierto, los riesgos de seguridad asociados a ellos cobran mayor relevancia»*, concluyeron los investigadores.

> *«La responsabilidad principal de asegurar a los usuarios recae en la plataforma. Es*

> *esencial que PowerShell Gallery y plataformas similares tomen medidas necesarias para fortalecer sus medidas de seguridad».*