Microsoft lanzó la segunda vista previa del Módulo de Administración de Secretos, un módulo de PowerShell para administrar secretos y credenciales.

La compañía presentó los Secretos de PowerShell en Ignite 2019 como una nueva forma de administrar se manera segura los secretos en entornos de nube que dependen de componentes de múltiples proveedores, como muchos proveedores de secretos.

El módulo proporciona un conjunto de cmdlets que permiten a los usuarios almacenar secretos de forma local mediante un proveedor de bóveda y acceder a los secretos de bóvedas remotas. Los usuarios pueden registrar y cancelar el registro de bóvedas locales y remotas en la máquina local para administrar y recuperar secretos. Microsoft lanzó la primera vista previa en febrero y ahora publicó la segunda vista previa.

Microsoft creó Secrets Management para abordar algunos desafíos que enfrentan los desarrolladores de PowerShell cuando los script avanzados requieren múltiples secretos para coordinarse en distintas nubes. El módulo de gestión de secretos admite varios tipos de secretos, incluidos PSCredential, SecureString, String, HashTable y Bye[].

La bóveda predeterminada en Windows es Credential Manager o CredMan, que se utiliza para autenticarse en una bóveda remota. Microsoft cree que podría ser útil al permitir que los desarrolladores ejecuten scripts en entornos locales, de prueba y de producción solo modificando la bóveda. En Linux, Microsoft planea utilizar GNOME Keyring mientras que en MacOS será Apple Keychain.

Las dos primeras vistas previas de PowerShell Secrets Management solo están disponibles para Windows, pero el soporte para Linux está planeado para la próxima vista previa, seguido del soporte de macOS.

Los usuarios que quieran instalar la segunda vista previa deberán reemplazar completamente el módulo y los módulos de extensión debido a los cambios importantes en esta versión.

Algunos de los cambios en la actualización incluyen nuevos nombres de cmdlet, por ejemplo, Add-Secret, que ahora se convierte en Set-Secret para reflejar su intención. Hay un nuevo cmdlet Test-Vault que permite a los propietarios de una extensión de bóveda verificar que esté configurado correctamente en el momento del registro.

Sydney Smith, un administrador de programas en el equipo de PowerShell de Microsoft, afirmó que los usuarios que instalaron la primera vista previa primero deben eliminar cualquier secreto de LocalDefaultVault antes de instalar la segunda vista previa.

> *«En función de los comentarios, cambiamos la convención de nomenclatura para los secretos almacenados en CredMan, por lo tanto, los secretos anteriores almacenados en la bóveda local ya no serán visibles luego de instalar la nueva versión del módulo»,* dijo Smith.

Sin embargo, los usuarios aún pueden ver y eliminar los viejos secretos a través de la interfaz de usuario de CredMan.

Smith proporcionó instrucciones para instalar la segunda vista previa desde una consola PowerShell en el blog para desarrolladores de PowerShell.