Se descubrió una vulnerabilidad de seguridad en Azure App Service de Microsoft, que resultó en la exposición del código fuente de las aplicaciones de los clientes escritas en Java, Node, PHP, Python y Ruby, durante al menos cuatro años desde septiembre de 2017.

La vulnerabilidad, con el nombre en código NotLegit, fue informada a la compañía por investigadores de Wiz el 7 de octubre de 2021, después de eso, se tomaron medidas para corregir el error de divulgación de información en noviembre.

Microsoft dijo que un *«subconjunto limitado de clientes»* está en riesgo, y dijo que *«los clientes que implementaron código en App Service Linux a través de Local Git después de que los archivos ya se crearon en la aplicación fueron los úincos clientes afectados».*

El Servicio de Aplicación Azure o Azure Web Apps, es una plataforma basada en la computación en la nube para la construcción y alojamiento de aplicaciones web. Permite a los usuarios implementar código fuente y artefactos en el servicio mediante un repositorio de Git local o mediante repositorios alojados en GitHub y Bitbucket.

El comportamiento predeterminado inseguro ocurre cuando se usa el método Local Git para implementar en Azure App Service, lo que da como resultado un escenario en el que el repositorio Git se crea dentro de un directorio de acceso público (home/site/wwwroot).

Aunque Microsoft agrega un archivo *«web.config»* a la carpeta .git, que contiene el estado y el historial del repositorio, para restringir el acceso público, los archivos de configuración solo se usan con aplicaciones C# o ASP.NET, que dependen de los propios servidores web IIS de Microsoft, dejando de lado las aplicaciones codificadas en otros lenguajes de programación como PHP, Ruby, Python o Node, que se implementan con diferentes servidores web como Apache, Nginx y Flask.

> *«Básicamente, todo lo que un actor malintencionado tenía que hacer era buscar en el directorio '/.git' de la aplicación de destino y recuperar su código fuente. Los actores malintencionados escanean continuamente Internet en busca de carpetas*

> *Git expuestas de las que puedan recopilar secretos y propiedad intelectual. Además de la posibilidad de que la fuente contenga secretos como contraseñas y token de acceso, el código fuente filtrado por lo general se utiliza para ataques más sofisticados»,* dijo el investigador de Wiz, Shir Tamari.