Microsoft lanzó Application Inspector, una herramienta de línea de comandos de código abierto multiplataforma que sus ingenieros utilizan para la investigación rápida de los componentes de software de código abierto de terceros en busca de problemas de seguridad.

El analizador de código fuente estático tiene como objetivo ayudar a los desarrolladores a manejar posibles problemas de seguridad que surgen por medio de la reutilización del código al incorporar componentes de código abierto, como bibliotecas de software, en algún proyecto.

> *«La reutilización tiene grandes beneficios, incluido el tiempo de comercialización, calidad e interoperabilidad, pero a veces conlleva el costo de la complejidad y el riesgo ocultos»,* escribieron Guy Acosta y Michael Scovetta, miembros del equipo de Seguridad y Confianza del cliente de Microsoft.
>
> *«Confía en su equipo de ingeniería, pero el código que escriben a menudo representa solo una pequeña fracción de toda la aplicación. ¿Qué tan bien entiende lo que realmente hacen todos estos componentes externos de software?».*

La compañía afirma que las aplicaciones web modernas, por lo general tienen cientos de componentes de terceros que contienen decenas de miles de líneas de código, que fueron escritas por miles de colaboradores. Y, por lo general, los desarrolladores que utilizan estos componentes confían en la descripción del autor, que Microsoft argumenta que no es confiable o suficiente para cumplir con la responsabilidad de Microsoft de enviar un código seguro, que incluye componentes externos.

La compañía también indica que Application Inspector es un analizador de código estático único porque no marca patrones *«buenos o malos»*, sino que destaca características interesantes en un informe basado en más de 500 patrones de reglas. La idea es que la herramienta pueda ayudar a identificar estas características interesantes más rápidamente

que la introspección manual.

La herramienta apunta a las características de los componentes de software que afectan la seguridad, como el uso de la criptografía, los componentes que se conectan a una entidad remota, como una nube pública, y las plataformas en las que se ejecuta.

Application Inspector se basa en .NET Core, lo que significa que los desarrolladores pueden utilizarlo en Windows, Linux o MacOS.

> *«El objetivo principal de Application Inspector es identificar las características del código fuente de una forma sistemática y escalable que no se encuentra en ningún otro lugar en los analizadores estáticos típicos. Esto permite a los desarrolladores y profesionales de seguridad, validar los objetivos de los componentes, por ejemplo, una biblioteca de relleno de cadenas solo hace lo que dice»,* explica Microsoft.

La herramienta puede analizar millones de líneas de código fuente de componentes que están construidos en múltiples lenguajes de programación populares.

Application Inspector produce un informe basado en el navegador que resumen las principales características identificadas, incluyendo los marcos de las aplicaciones, las interfaces en la nube, la criptografía, los datos confidenciales como claves de acceso, la información de identificación personal, las funciones del sistema operativo y las características de seguridad.

Microsoft enfatiza que Application Inspector no elimina la necesidad de revisar el código de seguridad o un analizador estático de seguridad. Sin embargo, podría ser una adición útil para los desarrolladores que enfrentan plazos ajustados.

Acosta demostró recientemente el Inspector de Aplicaciones en la conferencia SecTor en Canadá.