La Oficina Federal de Investigaciones (FBI), envió una alerta de seguridad en la que advierte que piratas informáticos están abusando de las aplicaciones SonarQube mal configuradas para acceder y robar repositorios de código fuente de agencias gubernamentales y empresas privadas de Estados Unidos.

Las intrusiones han tenido lugar desde al menos abril de 2020, según informó el FBI en una alerta enviada el mes pasado y hecha pública esta semana en su sitio web.

La alerta envía una advertencia específicamente a los propietarios de SonarQube, una aplicación basada en web que las empresas integran en sus cadenas de desarrollo de software para probar el código fuente y descubrir fallas de seguridad antes de implementar el código y las aplicaciones en entornos de producción.

Las aplicaciones SonarQube se instalan en servidores web y se conectan a sistemas de alojamiento de código fuente como cuentas de BitBucket, GitHub o GitLab, o sistemas Azure DevOps.

Pero el FBI afirma que algunas compañías han dejado estos sistemas desprotegidos, ejecutándose en su configuración predeterminada (en el puerto 9000), con credenciales de administrador predeterminadas.

Los funcionarios del FBI dicen que los actores de amenazas han abusado de estas configuraciones erróneas para acceder a las instancias de SonarQube, cambiar a los repositorios de código fuente conectados y luego acceder y robar aplicaciones patentadas o privadas/sensibles.

> *«En agosto de 2020, los actores de amenazas desconocidos filtraron datos internos de dos organizaciones a través de una herramienta de repositorio de ciclo de vida público. Los datos robados se obtuvieron de instancias de SonarQube que usaban configuraciones de puerto predeterminadas y credenciales de administrador que se ejecutaban en las redes de las organizaciones afectadas»,* dijo el FBI.

> *«Esta actividad es similar a una filtración de datos anterior en julio de 2020, en la que un actor cibernético identificado extrajo código fuente propietario de empresas a través de instancias de SonarQube mal aseguradas y publicó el código fuente extraído en un repositorio público autohospedado»,* agregó.

La alerta del FBI ha tocado un tema poco conocido entre los desarrolladores de software y los investigadores de seguridad.

Aunque la industria de la seguridad cibernética por lo general advierte sobre los peligros de dejar las bases de datos MongoDB o Elasticsearch expuestas en línea sin contraseñas, SonarQube se había mantenido alejada de las advertencias.

Sin embargo, algunos investigadores de seguridad han advertido sobre los peligros de dejar las aplicaciones SonarQube expuestas en línea con credenciales predeterminadas desde mayo de 2018.

Hasta ahora, el cazador de violaciones de datos, Bob Diachenko, advirtió que alrededor del 30% al 40% de las 3000 instancias aproximadamente de SonarQube disponibles en línea hasta ahora, no tenían ninguna contraseña o mecanismo de autenticación habilitado.

Este año, el investigador de seguridad suizo Till Kottmann, también planteó el mismo problema de instancias de SonarQube mal configuradas. A lo largo del año, Kottmann ha recopilado código fuente de decenas de empresas de tecnología en un portal público, y muchos de ellos provienen de aplicaciones SonarQube.

> *«La mayoría de la gente parece no cambiar absolutamente ninguna de las configuraciones, que en realidad se explican correctamente en la guía de configuración de SonarQube»*, dijo Kottmann.

> *«No sé el número actual de instancias de SonarQube expuestas, pero dudo que*

> *haya cambiado mucho. Supongo que todavía hay más de 1000 servidores que son vulnerables ya sea al no requerir autenticación o al dejarlos predeterminados»,* agregó.

Para evitar este tipo de fugas, la alerta del FBI enumera una serie de pasos que las empresas pueden tomar para proteger sus servidores SonarQube, comenzando por alterar la configuración y las credenciales predeterminadas de la aplicación y luego usando firewalls para evitar el acceso no autorizado a la aplicación.