Un investigador acusó a uno de los bancos más grandes de Canadá por *«seguridad de nivel muppet»*, luego de descubrir el código fuente de la aplicación y las claves de inicio de sesión privadas para los sistemas de back-end en los repositorios de GitHub.

La acusación proviene del profesional de TI, Jason Coulls, quien, según The Register, descubrió recientemente las carpetas de datos sin protección que pertenecen a Scotiabank.

«Estos repositorios presentaban, entre otras cosas, planos de software y claves de acceso para un sistema de tasa de cambio, código de aplicación móvil y credenciales de inicio de sesión para servicios e instancias de bases de datos». Describe los archivos como *«una potencial mina de oro de vulnerabilidades para que los delincuentes y hackers los exploten».*

Según el informe, Scotiabank pasó los últimos días derribando los repositorios de GitHub, que cree que se dejaron abiertos al público sin darse cuenta, después de que The Register se lo informara.

GitHub es un sitio de aloja un control de versión de software llamado Git, donde los desarrolladores pueden colaborar en las aplicaciones. Comprado por Microsoft el año pasado, se ha vuelto un servicio muy popular. Sin embargo, las organizaciones que permiten que el personal lo use deben asegurarse de que sus repositorios estén controlados con una contraseña sólida.

> *«Entre los cientos de archivos de documentación y código, que parecen haber sido creados por desarrolladores que trabajan en versiones de las aplicaciones móviles de Scotiabank para América Central y del Sur, había credenciales y claves para acceder a algunos de los sistemas y servicios de back-end del banco repartidos por todo el mundo. Entre los planos más sensibles estaba el código y los detalles de inicio de sesión para lo que parecía ser un sistema de base de datos SQL de tipos de cambio»,* dijo Coulls.

The Register citó a Coulls afirmando que entre las aplicaciones con sus credenciales

disponibles abiertamente, había una base de datos SQL Server con tasa de cambio. El código fuente al que se pudo acceder integró los sistemas del banco con los servicios de pago, incluyendo Samsung y Google Play, así como los procesadores de tarjetas de crédito estadounidenses Visa y Mastercard, entre otros.

Scotiabank no solo es usuario de GitHub, sino que también contribuye al ecosistema. El año pasado, el banco anunció su primera contribución de código abierto a la comunidad de GitHub para que los desarrolladores pueden usarla para sus aplicaciones.

Ilia Kolochenko, fundadora y directora ejecutiva de la compañía de seguridad web ImmuniWeb, dijo que los repositorios de códigos públicos, varios proyectos de código y de intercambio de datos, pueden facilitar en gran medida DevSecOps y acelerar el desarrollo ágil de software. Sin embargo, mencionó que traen un amplio espectro de riesgos comerciales críticos de fugas de datos inadvertidas o descuidadas, debido a la capacitación de seguridad insuficiente de los desarrolladores externos.

> *«Algunos desarrolladores comparten imprudentemente contraseñas de sistemas de producción en Pastebin, abriendo así las puertas a sus reinos digitales sin pensar en las consecuencias. Los cibercriminales son conscientes de la situación y rastrean de forma continua las fuentes de datos de acceso público para obtener un código fuente sensible, credenciales codificadas y claves API. Lo peor, a menudo tienen éxito y sus intrusiones con frecuencia permanecen sin ser detectadas ya que prácticamente no ocurren actividades anormales»,* dijo Kolochenko.

> *«Las grandes empresas necesitan diseñar cuidadosamente una política segura de desarrollo de software, y aplicarla y monitorearla adecuadamente. La capacitación periódica en seguridad para desarrolladores debería ser una parte esencial de la política. Se debe prestar especial atención cuando los desarrolladores se subcontratan a terceros que no están familiarizados con los procedimientos de seguridad y las mejores prácticas»,* agregó.