Investigadores de seguridad cibernética descubrieron un nuevo ataque app-in-the-middle, que podría permitir que una app maliciosa instalada en un dispositivo iOS robe información confidencial de otras aplicaciones al explotar algunas implementaciones del Esquema de URL Personalizado.

De forma predeterminada, en el sistema operativo iOS de Apple, cada aplicación se ejecuta dentro de una sandbox propia, lo que impide que todas las aplicaciones instaladas en el mismo dispositivo accedan a los datos de la otra.

Sin embargo, Apple ofrece algunos métodos que facilitan el envío y la recepción de datos muy ilimitados entre aplicaciones.

Uno de estos mecanismos se llama Esquema de URL, también conocido como Enlace Profundo, que permite a los desarrolladores lanzar aplicaciones por medio de URL, como facetime://, whatsapp://, fb-messenger://.

Por ejemplo, al hacer clic en *«Iniciar sesión con Facebook»* dentro de una app de comercio electrónico, inicia directamente la aplicación de Facebook instalada en su dispositivo y procesa automáticamente la autenticación.

En el fondo, esa aplicación de comercio electrónico activa el esquema de URL para la aplicación de Facebook y pasa cierta información de contexto requerida para procesar su inicio de sesión.

Los investigadores de Trend Micro notaron que ya que Apple no define explícitamente qué aplicación puede usar qué palabras clave para su Esquema de URL Personalizado, múltiples apps en un dispositivo iOS pueden usar un esquema de URL único, que eventualmente podría activar y pasar datos confidenciales a una aplicación completamente diferente de forma inesperada o maliciosa.

> *«Esta vulnerabilidad es particularmente crítica si el proceso de inicio de sesión de la*

> *aplicación A está asociado con la aplicación B»*, dijeron los investigadores.

Para demostrarlo, los investigadores ilustraron un escenario de ataque, como se observa en la siguiente imagen, utilizando un ejemplo de la aplicación china Suning y su implementación de la función *«Iniciar sesión con WeChat».*

Entonces, cuando los usuarios de la app Suning eligen acceder a su cuenta de comercio electrónico mediante WeChat, se genera una solicitud de inicio de sesión y la envía a la aplicación WeChat instalada en el mismo dispositivo mediante el esque de URL de iOS para la aplicación de mensajería. La app WeChat luego solicita un token de inicio de sesión secreto de su servidor y lo envía de regreso a la aplicación Suning para su autenticación.

Los investigadores descubrieron que, dado que Suning siempre usa la misma consulta de solicitud de inicio de sesión para solicitar el token secreto y WeChat no autentica la fuente de la solicitud de inicio de sesión, la implementación es vulnerable al ataque de la aplicación en el medio a través del esquema de URL de iOS. Finalmente, permite que los atacantes obtengan acceso no autorizado a las cuentas de los usuarios.

> *«Con el esquema de URL WeChat legítimo, se puede crear un WeChat falso, y Suning consultará el falso para el token de inicio de sesión. Si la aplicación Suning envía la consulta, entonces la aplicación falsa puede capturar su esquema de URL de solicitud de inicio de sesión. WeChat lo reconoce, pero no autenticará la fuente de la solicitud de inicio de sesión. En su lugar, responderá directamente con una señal de inicio de sesión a la fuente de la solicitud. Desafortunadamente, la fuente podría ser una aplicación maliciosa que está abusando del Esquema de URL de Suning»,* dijeron los investigadores.

Eso significa que la aplicación malintencionada con el mismo Esquema de URL Personalizado

que una app específica, puede engañar a otras aplicaciones para que compartan datos confidenciales de los usuarios con ella o puede realizar acciones no autorizadas, lo que podría resultar en la pérdida de privacidad, fraude de facturas o exposición a pop-ups de anuncios.

> *«En nuestra investigación, se encontraron muchas aplicaciones que nuestro sistema auditó, aprovechando esta función para mostrar anuncios a las víctimas. Las aplicaciones potencialmente maliciosas reclamarían intencionalmente el esquema de URL asociado con las aplicaciones populares. Identificamos algunas de estas aplicaciones maliciosas»*, agregaron.

Ya que la explotación de esta vulnerabilidad depende totalmente de la forma en que se ha implementado un esquema de URL, se recomienda a los desarrolladores de aplicaciones y plataformas populares que revisen sus aplicaciones y validen la corrección de solicitudes no confiables.