Un investigador de seguridad asegura haber descubierto una vulnerabilidad sin parches en el servicio de transferencia de dinero PayPal, que podría permitir a los hackers engañar a las víctimas para que, sin saberlo, completen transacciones dirigidas al atacante con un solo clic.

El secuestro de clics, también llamado reparación de la interfaz de usuario, se refiere a una técnica en la que se engaña a un usuario involuntario para que haga clic en elementos aparentemente inofensivos de un sitio web, como botones, con el objetivo de descargar malware, redirigir a sitios web maliciosos o divulgar información confidencial.

Por lo general, esto se logra al mostrar una página invisible o un elemento HTML en la parte superior de la página visible, lo que da como resultado un escenario en el que se engaña a los usuarios haciéndoles creer que están haciendo clic en la página legítima cuando en realidad están haciendo clic en el elemento falso superpuesto.

> *«Por lo tanto, el atacante está 'secuestrando' los clics destinados a la página [legítima] y los enruta a otra página, probablemente propiedad de otra aplicación, dominio o ambos»,* dijo el investigador h4x0r_dz.

H4x0r_dz, quien descubrió el problema en el punto final *«www.paypal[.]com/agreements/approve»,* dijo que el problema se informó a la empresa desde octubre de 2021.

> *«Este punto final está diseñado para acuerdos de facturación y solo debe aceptar billingAgreementToken. Pero durante mis pruebas profundas, descubrí que podemos pasar otro tipo de token, y esto conduce al robo de dinero de la cuenta de PayPal de la víctima»,* explicó el investigador.

Esto significa que un adversario podría incrustar el punto final antes mencionado dentro de

un iframe, lo que haría que una víctima que ya inició sesión en un navegador web transfiera fondos a una cuenta de PayPal controlada por el atacante simplemente haciendo clic en un botón.

Lo que es aún más preocupante, el ataque podría haber tenido consecuencias desastrosas en los portales en línea que se integran con PayPal para pagar, permitiendo al actor malicioso deducir montos arbitrarios de las cuentas de PayPal de los usuarios.

> *«Hay servicios en línea que permiten agregar saldo a su cuenta mediante PayPal. ¡Puedo usar el mismo exploit y obligar al usuario a entregar dinero a mi cuenta, o puedo explotar este error y dejar que la víctima cree/pague una cuenta de Netflix por mí!»,* dijo h4x0r_dz.