Apple pagó recientemente al investigador de vulnerabilidades indio, Bhavuk Jain, una recompensa de 100,000 dólares por informar sobre una vulnerabilidad crítica que afecta el sistema *«Iniciar sesión con Apple».*

La vulnerabilidad ahora parcheada podría haber permitido a los atacantes remotos eludir la autenticación y hacerse cargo de las cuentas de los usuarios específicos en servicios y aplicaciones de terceros que se han registrado utilizando la opción «Iniciar sesión con Apple».

Lanzado el año pasado en la conferencia WWDC de Apple, la función «Iniciar sesión con Apple» se introdujo en el mundo como un mecanismo de inicio de sesión para preservar la privacidad que permite a los usuarios registrar una cuenta con aplicaciones de terceros sin revelar sus direcciones de correo electrónico reales.

Bhavuk Jain reveló que la vulnerabilidad que descubrió residía en la forma en que Apple validaba a un usuario en el lado del cliente antes de iniciar una solicitud de los servidores de autenticación de Apple.

Al autenticar a un usuario a través de «Iniciar sesión con Apple», el servidor genera JSON Web Token (JWT), que contiene información secreta que la aplicación de terceros utiliza para confirmar la identidad del usuario que inicia sesión.

Bhavuk descubrió que, aunque Apple pide a los usuarios que inicien sesión en su cuenta de Apple antes de iniciar la solicitud, no estaba validando si la misma persona solicita JSON Web Token en el siguiente paso desde su servidor de autenticación.

Por lo tanto, la validación faltante es esa parte del mecanismo podría haber permitido que un atacante proporcione una ID de Apple separada perteneciente a una víctima, engañando a los servidores de Apple para que generen una carga útil JWT que sea válida para el inicio de sesión en un servicio de terceros con la identidad de la víctima.

> *«Descubrí que podía solicitar JWT para cualquier ID de correo electrónico de Apple, y cuando se verificó la firma de estos tokens utilizando la clave pública de Apple, se mostraron como válidos. Esto significa que un atacante podría falsificar un JWT al vincular cualquier ID de correo electrónico y obtener acceso a la cuenta de la víctima»*, dijo el investigador.

También confirmó que la vulnerabilidad funcionó incluso al elegir ocultar el ID de correo electrónico de los servicios de terceros y también puede ser explotada para registrar una nueva cuenta con la ID de Apple de la víctima.

> *«El impacto de esta vulnerabilidad fue bastante crítico ya que podría haber permitido una toma de control completa de la cuenta. Muchos desarrolladores han integrado iniciar sesión con Apple, ya que es obligatorio para las aplicaciones que admiten otros inicios de sesión sociales. Por nombrar algunos que usan Iniciar sesión con Apple: Dropbox, Spotify, Airbnb, Giphy»*, agregó Bhavuk.

Aunque la vulnerabilidad existía en el lago del código de Apple, el investigador dijo que es posible que algunos servicios y aplicaciones que ofrecen «Iniciar sesión con Apple» para sus usuarios ya hayan estado utilizando un segundo factor de autenticación que podría mitigar el problema para sus usuarios.

Bhavuk informó de forma responsable el problema al equipo de seguridad de Apple el mes pasado, y la compañía ahora corrigió la vulnerabilidad.

Además de pagar la recompensa por errores al investigador, en respuesta, la compañía también confirmó que investigó los registros de sus servidores y descubrió que la falla no fue explotada para comprometer ninguna cuenta.