Una popular plataforma de vieojuegos utilizada por cientos de millones de personas en todo el mundo, es vulnerable a múltiples fallas de seguridad que podrían haber permitido a los piratas informáticos remotos tomar las cuentas de los jugadores y robar datos confidenciales.

Las vulnerabilidades en cuestión residen en la plataforma de distribución digital «Origin», desarrollada por Electronic Arts (EA), la segunda compañía de juegos más grande del mundo, con más de 300 millones de usuarios, que permite a los usuarios comprar y jugar algunos de los vudeojuegos más populares, como Battlefield, Apex Legends, Madden NFL y FIFA.

La plataforma Origin también administra la autenticación de cuenta de los usuarios de EA Games, y les permite encontrar amigos, unirse a juegos y administrar sus perfiles.

Descubiertas por investigadores en Check Point y CyberInt, las vulnerabilidades cuando se encadenan podrían haber permitido a los atacantes secuestrar la cuenta de EA del jugador simplemente convenciéndolos de que abran una página web oficial desde el sitio web de EA Games.

Para realizar el ataque, como se muestra en el siguiente video, los investigadores aprovecharon una debilidad no parcheada conocida en el servicio de nube Azure de Microsoft, que les permitió tomar el control de uno de los subdominios de EA, que anteriormente estaba registrado en Azure para albergar uno de los servicios.

Como se explicó en un informe anterior, si el DNS (CNAME) de un dominio o subdominio apunta a la plataforma en la nube de Azure, pero no se ha configurado o vinculado a una cuenta de Azure activa, cualquier otro usuario de Azure puede secuestrarlo para estacionar ese subdominio en su servidor de Azure.

> *«Sin embargo, durante la investigación de Cyber Int, se descubrió que el servicio ea-invite-reg.azurewebsites.net ya no estaba en uso dentro de los servicios en la nube de Azure. Sin embargo, el único subdominio eaplayinvite.ea.com todavía redirigie a él utilizando la configuración de CNAME»,* dijeron los investigadores de

> CheckPoint.

En su ataque de prueba de concepto, los investigadores secuestraron *«eaplayinvite.ea.com»* y presentaron un script en él que aprovechaba las vulnerabilidades en el inicio de sesión único (SSO) de los juegos de EA y el mecanismo TRUST.

La página web finalmente permitió a los investigadores capturar tokens secretos de SSO de los jugadores con solo convencerlos de que los visitaran en el mismo navegador web en el que ya tienen una sesión activa en el sitio web de EA y tomar sus cuentas sin requerir credenciales reales.

> *«El mecanismo TRUST existe entre los dominios ea.com y origin.com y sus subdominios. Abusar con éxito del mecanismo permitió a nuestro equipo de investigación manipular la implementación del protocolo OAuth para una explotación completa de la adquisición de la cuenta»,* explicaron los investigadores.

En el peor de los casos, los investigadores de CheckPoint dijeron que un atacante podría haber explotado estas fallas para causar daños potenciales, como obtener acceso a la información de la tarjeta de crédito de los jugadores con la capacidad de comprar de forma fraudulenta la moneda del juego en nombre de los jugadores.

CyberInt y Check Point informaron inmediatamente de sus hallazgos a EA Games y ayudaron a la compañía a solucionar las lagunas de seguridad para proteger a sus clientes de juegos. La firma de seguridad se hizo pública hoy con sus hallazgos, casi tres meses después de que EA abordara dichos problemas.