Luego de una serie de problemas de seguridad y abuso de datos por medio de su plataforma de redes sociales, Facebook amplió hoy su programa de recompensas de errores de una forma única para reforzar la seguridad de las aplicaciones y sitios web de terceros que se integran con su plataforma.

El año pasado, Facebook lanzó el programa *«Data Abuse Bounty»*, para recompensar a quien informe sobre eventos válidos de aplicaciones de terceros que recopilan datos de usuarios de Facebook y los pasan a compañías maliciosas, violando así las políticas de datos renovadas de Facebook.

Aparentemente, la mayoría de las veces, los datos de los usuarios de Facebook que fueron mal utilizados, se expusieron en primer lugar como resultado de una vulnerabilidad o debilidad de seguridad en aplicaciones o servicios de terceros.

Facebook cuenta con millones de aplicaciones de terceros, y muy pocas de ellas tienen un programa de divulgación de vulnerabilidades u ofrecen recompensas por errores a los hackers de sombrero blanco por informar de forma responsable los errores en su base de código.

Debido a esta brecha de comunicación entre los investigadores y los desarrolladores de aplicaciones afectados, los programas de seguridad de Facebook para aplicaciones y sitios web de terceros estaban, hasta ahora, limitados a *«observar pasivamente las vulnerabilidades».*

Aunque Facebook ya expandió su programa de recompensas de errores para aplicaciones de terceros a finales del año pasado, el esquema solo se limitó a la presentación de informes válidos para la exposición de los tokens de acceso de los usuarios de Facebook que permiten a las personas iniciar sesión en otra app utilizando Facebook.

Esfuerzos para aumentar la colaboración entre hackers y

desarrolladores

Para que los desarrolladores de aplicaciones de terceros se sientan más comprometidos a tomar más en serio la seguridad de sus aplicaciones y establezcan un programa de divulgación de vulnerabilidades, Facebook decidió pagar a los investigadores de su propio dinero, incluso si los desarrolladores de aplicaciones no tienen su propio programa de recompensas.

> *«Aunque estos errores no están relacionados con nuestro propio código, queremos que los investigadores tengan un canal claro para informar estos problemas si pudieran hacer que los datos de nuestros usuarios pudieran ser mal utilizados».* dijo Facebook.
>
> *«También queremos incentivar a los investigadores para que se centren en aplicaciones, sitios web y programas de recompensas por errores que de otra forma no recibirían tanta atención o no tendrían recursos para incentivar a la comunidad de recompensas de errores. Al comprometernos a recompensar informes válidos sobre errores en aplicaciones y sitios web de terceros que afectan los datos de Facebook, esperamos alentar a la comunidad de seguridad a interactuar con más desarrolladores de aplicaciones»,* agregó la compañía.

Los desarrolladores de aplicaciones pueden aprovechar este programa simplemente configurando su propia política de divulgación de vulnerabilidad, que luego ayudaría a los investigadores a ser elegibles para encontrar errores en su código y reclamar recompensas de Facebook.

Esto se debe a que un informe acerca de una vulnerabilidad en aplicaciones de terceros enviadas a Facebook solo se considerará válido cuando los investigadores incluyan una prueba de autorización otorgada por el desarrollador externo al enviar sus informes al programa de recompensas de errores de Facebook.

Sin embargo, si los desarrolladores de terceros ya tienen su propio programa de recompensas de errores, los investigadores pueden reclamar recompensas de ambas partes.

La recompensa de Facebook se emitirá dependiendo del impacto potencial y la gravedad de la vulnerabilidad informada responsablemente, con un pago mínimo de 500 dólares.

Los programas de recompensas de errores por abuso de datos y aplicaciones de terceros que afectan a todo el ecosistema son una tendencia creciente en seguridad cibernética.

Google es otra compañía que también amplió su programa de recompensas Pay Store para recompensar a los hackers por encontrar errores en cualquier app de Android que tenga más de 100 millones de descargas.