La Agencia de Segurida de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó dos vulnerabilidades a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), según evidencia de explotación activa.

Las dos vulnerabilidades son las siguientes:

- CVE-2023-20963 (puntaje CVSS: 7.8): Vulnerabilidad de escalada de privilegios del marco de trabajo en Android.
- CVE-2023-29492 (puntaje CVSS: TBD): Vulnerabilidad de deserialización insegura de la encuesta de Novi.

> *«Android Framework contiene una vulnerabilidad no especificada que permite la escalada de privilegios después de actualizar una aplicación a un SDK de destino superior sin necesidad de privilegios de ejecución adicionales»,* dijo CISA en un aviso para CVE-2023-20963.

Google, en su boletín de seguridad de Android mensual para marzo de 2023, reconoció que *«hay indicios de que CVE-2023-20963 puede estar bajo explotación limitada y dirigida».*

El desarrollo se produce cuando el sitio de noticias tecnológicas Ars Technica reveló a fines del mes pasado que las aplicaciones de Android firmadas digitalmente por la empresa de comercio electrónico de China, Pinduoduo, usaron la vulnerabilidad como un arma de día cero para tomar el control de los dispositivos y robar datos confidenciales, citando un análisis de seguridad móvil de la compañía Lookout.

La principal de las capacidades de la aplicación con malware incluye inflar la cantidad de usuarios activos diarios mensuales de Pinduoduo, desinstalar aplicaciones rivales, acceder a notificaciones e información de ubicación, y evitar que se desinstale.

CNN, en un informe de seguimiento publicado a inicios del mes, dijo que un análisis de la versión 6.49.0 de la aplicación, reveló un código diseñado para lograr una escalada de

privilegios e incluso rastrear la actividad del usuario en otras aplicaciones de compras.

Los exploits permitieron que la aplicación maliciosa accediera a los contactos, calendarios y álbumes de fotos de los usuarios sin su consentimiento, y solicitaron una *«gran cantidad de permisos más allá de las funciones normales de una aplicación de compras»,* dijo el canal de noticias.

Cabe mencionar que Google suspendió la aplicación oficial de Pinduoduo de Play Store en marzo, citando malware identificado en *«versiones fuera de Play»* del software.

Aún no está claro cómo se firmaron estos archivos APK con la misma clave usada para firmar la aplicación legítima de Pinduoduo. Esto apunta a una fuga de clave, el trabajo de un infiltrado deshonesto, un compromiso de la canalización de compilación de Pinduoduo o un intento deliberado de la empresa china de distribuir malware.

La segunda vulnerabilidad agregada al catálogo KEV se relaciona con una vulnerabilidad de deserialización insegura en el software Novi Survey, que permite a atacantes remotos ejecutar código en el servidor en el contexto de la cuenta de servicio.

El problema, que afecta a las versiones de Novi Survey anteriores a la 8.9.43676, fue abordado por el proveedor con sede en Boston a inicios de esta semana el 10 de abril de 2023. Actualmente no se sabe cómo se abusa de la vulnerabilidad en los ataques del mundo real.

Para contrarrestar los riesgos que generan las vulnerabilidades, se recomienda a las agencias del Poder Ejecutivo Federal Civil (FCEB) de Estados Unidos, que apliquen los parches necesarios antes del 4 de mayo de 2023.