Google anunció este martes la disponibilidad de la herramienta de código abierto OSV-Scanner, un escáner que tiene como objetivo ofrecer un fácil acceso a la información de vulnerabilidad sobre varios proyectos.

La herramienta basada en Go, impulsada por la base de datos de vulnerabilidades de código abierto (OSV), está diseñada para conectar *«la lista de dependencias de un proyecto con las vulnerabilidades que las afectan»*, dijo el ingeniero de software de Google, Rex Pan.

> *«OSV-Scanner genera información de vulnerabilidad confiable y de alta calidad que cierra la brecha entre la lista de paquetes de un desarrollador y la información en las bases de datos de vulnerabilidades»,* agregó Pan.

El objetivo es identificar todas las dependencias transitivas de un proyecto y resaltar las vulnerabilidades relevantes usando datos extraídos de la base de datos OSV.dev.

Google declaró además que la plataforma de código abierto admite 16 ecosistemas, contando todos los principales idiomas, distribuciones de Linux (Debian y Alpine), así como Android, Linux Kernel y OSS-Fuzz.

El resultado de esta expansión es que OSV.dev es un repositorio de más de 38,000 avisos, frente a las 15,000 alertas de seguridad de hace un año, con Linux (27.4%), Debian (23.2%), PyPI (9.5%), Alpine (7.9%) y npm (7.1%) ocupando los cinco primeros puestos.

En cuanto a los siguientes pasos, la compañía de Internet dijo que está trabajando para incorporar soporte para fallas de C/C++ mediante la creación de una *«base de datos de alta calidad»* que implica agregar *«metadatos de nivel de confirmación precisos a CVE».*

OSV-Scanner llega casi dos meses después de que Google lanzara GUAC, abreviatura de

Graph for Understanding Artifact Composition, para complementar los niveles de cadena de suministro par artefactos de software (SLSA) como parte de sus esfuerzos para fortalecer la seguridad de la cadena de suministro de software.

La semana pasada, Google también publicó un nuevo informe «Perspectivas sobre la seguridad» en el que se pide a las organizaciones que desarrollen e implementen un marco SLSA común para evitar la manipulación, mejorar la integridad y proteger los paquetes contra posibles amenazas.

Otras recomendaciones presentadas por la empresa incluyen asumir responsabilidades adicionales de seguridad de código abierto y adoptar un enfoque más holístico para abordar riesgos como los presentados por la vulnerabilidad Log4j y el incidente de SolarWinds en los últimos años.

> *«Los ataques a la cadena de suministro de software por lo general requieren una gran aptitud técnica y un compromiso a largo plazo para mejorarlo. Es más probable que los actores sofisticados tengan tanto la intención como la capacidad de realizar este tipo de ataques»,* dijo la compañía.

> *«La mayoría de las organizaciones son vulnerables a los ataques de la cadena de suministro de software porque los atacantes se toman el tiempo para apuntar a proveedores externos con conexiones confiables a las redes de sus clientes. Luego usan esa confianza para profundizar en las redes de sus objetivos finales».*