Google lanzó una nueva versión de Scorecards, su herramienta de seguridad automatizada que produce una *«puntuación de riesgo»* para iniciativas de código abierto, con comprobaciones y capacidades mejoradas para hacer que los datos generados por la utilidad sean accesibles para su análisis.

> *«Con tanto software hoy en día que depende de proyectos de código abierto, los consumidores necesitan una forma fácil de juzgar si sus dependencias son seguras. Los cuadros de mando ayudan a reducir el trabajo y el esfuerzo manual necesarios para evaluar de forma continua los cambios de paquetes al mantener la cadena de suministro de un proyecto»*, dijo el equipo de seguridad de código abierto de Google.

Scorecards tiene como objetivo automatizar el análisis de la postura de seguridad de los proyectos de código abierto, además de utilizar las métricas de salud de seguridad para mejorar de forma proactiva la postura de seguridad de otros proyectos críticos. Hasta ahora, la herramienta se ha ampliado para evaluar los criterios de seguridad para más de 50 mil proyectos de código abierto.

Algunas de las nuevas incorporaciones incluyen comprobaciones de contribuciones de autores malintencionados o cuentas comprometidas que pueden introducir posibles puertas traseras en el código, uso de fuzzing como OSS-Fuzz, y herramientas de análisis de código estático, como CodeQL, signos de compromiso CI/CD y malas dependencias.

> *«Anclar dependencias es útil en todos los lugares donde tenemos dependencias: no solo durante la compilación, sino también en Dockerfiles, flujos de trabajo CI/CD, etc. Las tarjetas de puntuación comprueban estos antipatrones con la comprobación Frozen-Deps. Esta comprobación es útil para mitigar los ataques de dependencia maliciosos, como el reciente ataque CodeCov»*, dijo el equipo.

Google también dijo que una gran cantidad de proyectos analizados no se borran de forma continua, y que ni definen una política de seguridad para informar vulnerabilidades ni fijan dependencias, al mismo tiempo que hace énfasis en la necesidad de mejorar la seguridad de estos proyectos críticos y generar conciencia de los riesgos de seguridad generalizados.

El lanzamiento de Scorecards v2 se produce semanas después de que la compañía presentara un marco de trabajo integral llamado *«Niveles de cadena de suministro para artefactos de software»* (SLSA) para garantizar la integridad de los artefactos de software y evitar modificaciones no autorizadas durante el desarrollo y la implementación.