Google anunció el jueves un conjunto de iniciativas destinadas a mejorar el ecosistema de gestión de vulnerabilidades y establecer mayores medidas de transparencia en torno a la explotación.

> *«Aunque la notoriedad de las vulnerabilidades de día cero generalmente aparecen en los titulares, los riesgos permanecen incluso después de que se conocen y solucionan, que es la historia real. Esos riesgos abarcan todo, desde el tiempo de retraso en la adopción de OEM, los puntos débiles de las pruebas de parches, los problemas de actualización del usuario final y más»*, dijo la compañía en un anuncio.

Las amenazas de seguridad también provienen de parches incompletos aplicados por los proveedores, con una parte de los días cero explotados en la naturaleza que resultan ser variantes de vulnerabilidades parcheadas previamente.

Mitigar dichos riesgos requiere abordar la causa raíz de las vulnerabilidades y priorizar las prácticas modernas de desarrollo de software seguro para eliminar clases enteras de amenazas y bloquear posibles vías de ataque.

Teniendo en cuneta estos factores, Google dijo que está formando un Consejo de Políticas de Hacking junto con Bugcrowd, HackerOne, Intel, Intigriti y Luta Security para *«garantizar que las nuevas políticas y regulaciones respalden las mejores prácticas para la gestión y divulgación de vulnerabilidades».*

La compañía enfatizó además que se compromete a divulgar públicamente los incidentes cuando encuentre evidencia de explotación activa de vulnerabilidades en su cartera de productos.

Finalmente, la compañía dijo que está instituyendo un Fondo de Defensa Legal de Investigación de Seguridad para proporcionar fondos iniciales para la representación legal de las personas que participan en investigaciones de buena fe para encontrar e informar

vulnerabilidades de una forma que avance la ciberseguridad.

El objetivo, dijo la compañía, es escapar del *«bucle fatal»* del parcheo de vulnerabilidades y la mitigación de amenazas al *«centrarse en los fundamentos del desarrollo de software seguro, una buena higiene de los parches y el diseño para la seguridad y facilidad de los parches desde el principio».*

El último impulso de seguridad de Google habla de la necesidad de mirar más allá de los días cero al dificultar la explotación en primer lugar, impulsar la adopción de parches para vulnerabilidades conocidas de forma oportuna, establecer políticas para abordar los ciclos de vida del producto y hacer que los usuarios sean conscientes cuando los productos son explotados activamente.

También sirve para resaltar la importancia de aplicar principios de seguridad desde el diseño durante todas las fases del ciclo de vida del desarrollo de software.

La divulgación se produce cuando Google lanzó un servicio de API gratuito llamado API deps.dev en un intento por proteger la cadena de suministro del software al proporcionar acceso a metadatos de seguridad e información de dependencia para más de 50 millones de versiones de cinco millones de paquetes de código abierto que se encuentran en Go, Maven, PyPI, npm y repositorios Cargo.

En un desarrollo relacionado, la división de la nube de Google también ha anunciado la disponibilidad general del servicio Assured Open Source Software (Assured OSS) para los ecosistemas de Java y Python.