Los encargados del mantenimiento de Composer, un administrador de paquetes para PHP, enviaron una actualización para abordar una vulnerabilidad crítica que podría haber permitido a un atacante ejecutar comandos arbitrarios y *«puerta trasera de todos los paquetes PHP»*, resultando en un ataque a la cadena de suministro.

Rastreada como CVE-2021-29472, la vulnerabilidad fue descubierta e informada el 22 de abril por investigadores de SonarSource, después de esto se implementó una revisión menos de 12 horas después.

> *«Se corrigió la vulnerabilidad de inyección de comandos en HgDriver/HgDownloader y se fortalecieron otros controladores y descargadores de VCS. Hasta donde sabemos, la vulnerabilidad no ha sido explotada»,* dijo Composer en sus notas de lanzamiento para las versiones 1.0.13 y 1.10.22.

Composer se promociona como una herramienta para la gestión de dependencias en PHP, lo que permite una fácil instalación de paquetes relevantes para un proyecto. También permite a los usuarios instalar aplicaciones PHP que están disponibles en Packagist, un repositorio que agrega todos los paquetes PHP públicos instalables con Composer.

Según SonarSource, la vulnerabilidad se debe a la forma en que se manejan las URL de descarga de la fuente del paquete, lo que podría conducir a un escenario en el que un adversario podría desencadenar la inyección de comandos remotos. Como prueba de este comportamiento, los investigadores aprovecharon la falla de la inyección de argumentos para crear una URL de repositorio de Mercurial maliciosa, que aprovecha su opción *«alias»* para ejecutar un comando de shell que elija el atacante.

> *«Una vulnerabilidad en un componente tan central, que atiende a más de 100 millones de solicitudes de metadatos de paquetes por mes, tiene un gran impacto, ya que este acceso podría haberse utilizado para robar las credenciales de los encargados de mantenimiento o para redirigir las descargas de paquetes a*

> *servidores de terceros que ofrecen dependencias con puertas traseras»,* dijo SonarSource.

La firma de seguridad de código con sede en Ginebra, dijo que uno de los errores se introdujo en noviembre de 2011, lo que sugiere que el código vulnerable acechaba desde el momento en que comenzó el desarrollo en Composer hace 10 años. La primera versión *«alfa»* de Composer se lanzó el 3 de julio de 2013.

> *«El impacto para los usuarios de Composer directamente es limitado, ya que el archivo composer.json generalmente está bajo su propio control y las URL de descarga de origen solo pueden ser proporcionadas por repositorios de Composer de terceros en los que confían explícitamente para descargar y ejecutar el código fuente, por ejemplo, complementos de Composer»*, dijo Jordi Boggiano, uno de los principales desarrolladores de Composer.