Se reveló una vulnerabilidad de seguridad de hace 15 años en el repositorio PHP de PEAR, que podría permitir a un atacante realizar ataques a la cadena de suministro, incluyendo la obtención de acceso no autorizado para publicar paquetes no autorizados y ejecutar código arbitrario.

> *«Un atacante que explote la primera vulnerabilidad podría apoderarse de cualquier cuenta de desarrollador y publicar lanzamientos maliciosos, mientras que el segundo error permitiría al atacante obtener acceso persistente al servidor PEAR central»,* dijo el investigador de vulnerabilidades de SonarSource, Thomas Chauchefoin.

PEAR, abreviatura de PHP Extension and Application Repository, es un marco y un sistema de distribución para componentes PHP reutilizables.

Una de las vulnerabilidades, introducida en una confirmación de código realizada en marzo de 2007, cuando la función se implementó originalmente, se relaciona con el uso de la función PHP criptográficamente insegura mt_rand() en la funcionalidad de restablecimiento de contraseña, que podría permitir a un atacante *«descubrir una contraseña válida y restablecer el token en menos de 50 intentos».*

Con este exploit, un atacante podría apuntar a las cuentas de administrador o desarrollador existentes para secuestrarlas y publicar nuevas versiones troyanizadas de paquetes que ya mantienen los desarrolladores, lo que resultaría en un compromiso generalizado de la cadena de suministro.

La segunda vulnerabilidad, que requiere que el adversario la encadene con la falla antes mencionada para lograr el acceso inicial, se deriva de la dependencia de pearweb de una versión anterior de Archive_Tar, que es susceptible a un error transversal de directorio de alta gravedad (CVE-2020-36193), lo que lleva a la ejecución de código arbitrario.

> *«Estas vulnerabilidades han estado presentes durante más de una década y fueron triviales de identificar y explotar, lo que genera dudas sobre la falta de contribuciones de seguridad de las empresas que dependen de ellas»,* dijo Chauchefoin.

Estos hallazgos marcan la segunda vez que se descubren problemas de seguridad en la cadena de suministro de PHP en menos de un año. A fines de abril de 2021, se divulgaron vulnerabilidades críticas en el administrador de paquetes Composer PHP, que podrían permitir que un adversario ejecute comandos arbitrarios.

Con los ataques a la cadena de suministro de software emergiendo como una amenaza peligrosa a raíz de los incidentes de protestware dirigidos a bibliotecas ampliamente utilizadas en el ecosistema NPM, los problemas de seguridad relacionados con las dependencias de código en el software vuelven a estar en el centro de atención, lo que llevó a Open Source Initiative a la «*militarización del código abierto*«, como un acto de vandalismo cibernético que *«supera cualquier beneficio posible».*