Un grave fallo de seguridad que afecta a la aplicación de intercambio de archivos de código abierto ProjectSend parece estar siendo explotado activamente, según un informe de VulnCheck.

La vulnerabilidad, que se corrigió inicialmente en mayo de 2023 mediante una actualización al código, no estuvo disponible de manera oficial hasta agosto de 2024 con la publicación de la versión r1720. A fecha del 26 de noviembre de 2024, este problema ha sido registrado con el identificador CVE-2024-11680 y una puntuación CVSS de 9.8.

El problema fue reportado en enero de 2023 por Synacktiv, que lo describió como una falla en los controles de autorización que permite a un atacante ejecutar código malicioso en servidores afectados.

> *«Se detectó un defecto en la verificación de autorización en la versión r1605 de ProjectSend, lo que permite que un atacante realice acciones críticas como activar el registro de usuarios y la validación automática o añadir extensiones permitidas en la lista blanca para archivos subidos»,* señaló Synacktiv en un informe publicado en julio de 2024.
>
> *«Esto, en última instancia, permite la ejecución de código PHP arbitrario en el servidor donde se encuentra instalada la aplicación.»*

Por su parte, VulnCheck ha identificado actividades de atacantes desconocidos que están aprovechando código de explotación publicado por Project Discovery y Rapid7 para comprometer servidores públicos de ProjectSend. Según las observaciones, los ataques comenzaron en septiembre de 2024.

Estos ataques incluyen la activación del registro de usuarios para conseguir privilegios posteriores a la autenticación y continuar con la explotación, lo que indica que no se limitan a buscar instancias vulnerables.

> *«Es probable que estemos en una etapa donde los atacantes están instalando shells web en los servidores»* (además, la vulnerabilidad también permite incrustar JavaScript malicioso, lo que podría dar lugar a un enfoque diferente de ataque), comentó Jacob Baines, de VulnCheck.
>
> *«Si un atacante sube un shell web, es posible encontrarlo en una ubicación predecible dentro de `upload/files/`, a partir de la raíz del servidor web.»*

Un análisis de los servidores de ProjectSend expuestos en internet mostró que solo un 1% está ejecutando la versión actualizada (r1750), mientras que el resto utiliza versiones más antiguas, incluida la r1605, que se lanzó en octubre de 2022.

Dado el aparente uso extendido de esta vulnerabilidad, se insta a los usuarios a aplicar las actualizaciones más recientes cuanto antes para protegerse de esta amenaza activa.