Alert Bulletin

Bulletin N.: 60
Publication Date: 17/07/2025
Subject: Alerta 2025-60 Vulnerabilidad Critica en componente de Laravel PHP
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- binarytorch/larecipe (Compositor) < 2.8.1

Descripción

Se ha reportado una vulnerabilidad altamente crítica de Server-Side Template Injection (SSTI)[1] en la librería LaRecipe, componente para documentación utilizado por el framework de desarrollo Laravel de PHP, potencialmente esta vulnerabilidad prodía afectar a millones de usuarios. La falla **CVE-2025-53833 (CVSSv3 10)** puede provocar la ejecución remota de código (RCE), lo que podría permitir a los atacantes tomar el control total de los servidores que ejecutan la versión afectada de LaRecipe.

LaRecipe es un paquete de Laravel basado en código que permite a los desarrolladores crear y gestionar fácilmente documentación atractiva directamente en sus aplicaciones. Se integra a la perfección en el ecosistema de Laravel y admite la creación de contenido basado en Markdown, el control de versiones y la personalización de temas. Con más de 2,3 millones de descargas, LaRecipe es una de las herramientas favoritas de los desarrolladores de Laravel para crear documentación integrada en la aplicación. Sin embargo, su popularidad podría convertirla en un blanco fácil para la explotación.

La causa principal de CVE-2025-53833 es una vulnerabilidad SSTI, lo que significa que los atacantes pueden inyectar código arbitrario en las plantillas del servidor de LaRecipe. Una vez renderizado, este código puede ejecutarse con los mismos privilegios que la propia aplicación.

Dependiendo de la configuración del servidor de destino, los atacantes podrían:

- Ejecutar comandos arbitrarios en el servidor
- Acceda a variables .env confidenciales, como credenciales de base de datos y claves API
- Aumentar los privilegios, lo que podría permitir obtener acceso root o administrativo

Solución:

Se recomienda a los desarrolladores y equipos de DevOps que actualicen a LaRecipe v2.8.1 o posterior, que contiene la corrección necesaria para eliminar esta vulnerabilidad SSTI.

Información adicional:

- https://securityonline.info/cve-2025-53833-cvss-10-critical-ssti-flaw-in-larecipe-threatens-millions-of-laravel-apps/

---

[1] La inyección de plantilla del lado del servidor es cuando un atacante puede usar la sintaxis de plantilla nativa para inyectar una carga maliciosa en una plantilla, que luego se ejecuta en el lado del servidor https://portswigger.net/web-security/server-side-template-injection .