BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-64
Fecha de publicación: 15/11/2024
Tema: vulnerabilidad critica cve-2024-52301 en Laravel
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Versiones < 6.20.45
- Versiones >= 7.0.0 y < 7.30.7
- Versiones >= 8.0.0 y < 8.83.28
- Versiones >= 9.0.0 y < 9.52.17
- Versiones >= 10.0.0 y < 10.48.23
- Versiones >= 11.0.0 y < 11.31.0

Descripción

Laravel es un framework de código abierto ampliamente utilizado para desarrollar aplicaciones y servicios web con PHP. Este framework es conocido por su sintaxis elegante y su conjunto de herramientas integradas que permiten construir aplicaciones robustas de manera eficiente.

Recientemente, se ha identificado una vulnerabilidad crítica, CVE-2024-52301, que afecta a varias versiones de Laravel. Esta vulnerabilidad representa un riesgo significativo para las aplicaciones creadas con Laravel, ya que puede permitir acceso no autorizado, manipulación de datos o escalada de privilegios.

El problema radica en una validación de entrada incorrecta que explota la configuración del entorno del framework. En concreto, la falla está relacionada con la directiva `register_argc_argv` de PHP, la cual permite procesar argumentos de la línea de comandos en scripts. Si esta directiva está habilitada, los atacantes pueden manipular el comportamiento de Laravel mediante URLs especialmente diseñadas, alterando las variables de entorno utilizadas para procesar solicitudes.

Este defecto proporciona a los atacantes una vía para eludir controles de validación o inyectar datos maliciosos. Aplicaciones que tienen activada la directiva `register_argc_argv`

son particularmente vulnerables, ya que esta configuración amplía la superficie de ataque al permitir que actores maliciosos exploten el comportamiento predeterminado de PHP.

Solución

Laravel ha emitido actualizaciones para resolver la vulnerabilidad **CVE-2024-52301**. Las versiones parcheadas son las siguientes:

- 6.20.45
- 7.30.7
- 8.83.28
- 9.52.17
- 10.48.23
- 11.31.0

Información adicional:

- https://github.com/advisories/GHSA-gv7v-rgg6-548h
- https://www.securityhive.io/blog/understanding-cve-2024-52301-why-you-must-upgrade-your-laravel-application
- https://securityonline.info/critical-laravel-flaw-cve-2024-52301-exposes-millions-of-web-applications-to-attack/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com