Una grave vulnerabilidad de seguridad que afecta al sistema de gestión de contenido (CMS) Craft ha sido incluida por la Agencia de Seguridad Cibernética y de Infraestructura de EE. UU. (CISA) en su lista de Vulnerabilidades Explotadas Conocidas (KEV), tras detectar pruebas de explotación activa.

El fallo de seguridad, identificado como CVE-2025-23209 (con una puntuación CVSS de 8.1), impacta las versiones 4 y 5 de Craft CMS. Los desarrolladores del proyecto resolvieron el problema a finales de diciembre de 2024 con las actualizaciones 4.13.8 y 5.5.8.

> *«Craft CMS presenta una vulnerabilidad de inyección de código que permite la ejecución remota de código, ya que las versiones afectadas han visto comprometidas las claves de seguridad de los usuarios»,* explicó la agencia.

Las versiones del software afectadas por este problema son:

- Desde 5.0.0-RC1 hasta antes de 5.5.5
- Desde 4.0.0-RC1 hasta antes de 4.13.8

En un comunicado publicado en GitHub, Craft CMS advirtió que todas las versiones sin actualizar con una clave de seguridad comprometida están expuestas a este defecto de seguridad.

> *«Si no es posible actualizar a una versión corregida, cambiar la clave de seguridad y garantizar su confidencialidad puede ayudar a reducir el riesgo»*, indicó el aviso.

Por ahora, no se ha determinado de qué manera se comprometieron las claves de seguridad de los usuarios ni en qué circunstancias. Para mitigar el riesgo que representa esta vulnerabilidad, se recomienda que las agencias de la Rama Ejecutiva Civil Federal (FCEB) implementen las correcciones necesarias antes del 13 de marzo de 2025.

En diciembre de 2024, Craft CMS también alertó sobre la explotación activa de otra vulnerabilidad (CVE-2024-56145), la cual podría permitir la ejecución remota de código si la configuración `register_argc_argv` de PHP está activada. Sin embargo, esta vulnerabilidad aún no ha sido agregada al catálogo KEV de CISA.