La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) ha incluido una vulnerabilidad crítica en Adobe ColdFusion en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) debido a pruebas de explotación activa.

Esta vulnerabilidad, identificada como CVE-2023-26359 (puntuación CVSS: 9.8), está relacionada con un fallo de deserialización presente en Adobe ColdFusion 2018 (Actualización 15 y versiones anteriores) y ColdFusion 2021 (Actualización 5 y versiones anteriores) que podría resultar en la ejecución de código arbitrario en el contexto del usuario actual sin requerir interacción alguna.

La deserialización (también conocida como «unmarshaling») se refiere al proceso de reconstruir una estructura de datos u objeto a partir de una secuencia de bytes. Sin embargo, cuando se realiza sin validar su fuente o depurar su contenido, puede llevar a consecuencias inesperadas, como la ejecución de código o ataques de denegación de servicio (DoS).

Adobe resolvió esta vulnerabilidad como parte de las actualizaciones lanzadas en marzo de 2023. Hasta el momento, no está claro cómo se está aprovechando esta vulnerabilidad en el mundo real.

Dicho esto, este desarrollo se produce más de cinco meses después de que CISA incluyera otra vulnerabilidad que afecta al mismo producto (CVE-2023-26360) en el catálogo KEV. Adobe ha informado que es consciente de que esta debilidad está siendo explotada en *«ataques muy limitados»* dirigidos a ColdFusion.

Debido a la explotación activa, se requiere que las agencias del Poder Ejecutivo Civil Federal (FCEB, por sus siglas en inglés) apliquen los parches necesarios antes del 11 de septiembre de 2023 para proteger sus redes contra posibles amenazas.