Una vulnerabilidad crítica de seguridad en Apache Roller, una plataforma de blogs de código abierto desarrollada en Java, está siendo explotada activamente en entornos reales, de acuerdo con información proporcionada por la Apache Software Foundation (ASF).

La falla, identificada como CVE-2026-129448 (con una puntuación CVSS de 9.8), corresponde a un problema de deserialización sin autenticación en el punto de acceso XML-RPC, cuya explotación podría permitir la ejecución remota de código.

Los responsables del proyecto señalaron que *«la deserialización de datos no confiables en las versiones de Apache Roller comprendidas entre la 4.0.0 y la 6.1.4 permite que un atacante remoto, sin necesidad de autenticarse, ejecute código arbitrario»*. Asimismo, explicaron que *«el endpoint XML-RPC admite tipos de extensión de proveedores y los deserializa antes de verificar la autenticidad del solicitante»*.

Por su parte, la ASF indicó que esta vulnerabilidad corresponde al mismo problema de seguridad registrado como CVE-2026-82384 (con una puntuación CVSS de 9.8), el cual recibió una corrección en septiembre de 2026 y cuya afectación se había atribuido únicamente a Apache Roller 6.1.5.

La fundación también confirmó que *«este problema está siendo explotado activamente»*. Sin embargo, no proporcionó información adicional sobre los métodos utilizados para aprovechar la vulnerabilidad ni sobre los posibles objetivos de estos ataques.

El hallazgo de esta falla fue atribuido al investigador de seguridad identificado como n0mi1k, mientras que Matt Raible recibió reconocimiento por haber presentado el reporte correspondiente.

Ante este escenario, se recomienda a los usuarios actualizar Apache Roller a la versión 6.1.6 o una posterior. Estas versiones deshabilitan los tipos de extensión y rechazan las solicitudes XML-RPC cuando dicha funcionalidad se encuentra inactiva.

En caso de que no sea posible instalar la actualización de manera inmediata, se aconseja

establecer el parámetro «enabledForExtensions» en «false» dentro del archivo WEB-INF/web.xml. Otra alternativa consiste en eliminar la asignación del servlet «/roller-services/xmlrpc» y posteriormente reiniciar el servicio Roller.

Finalmente, la ASF advirtió que *«desactivar XML-RPC desde la interfaz de administración no constituye una medida suficiente, debido a que las versiones anteriores realizan la deserialización de las solicitudes antes de comprobar el estado de dicha configuración»*.