Apache Roller Critical Flaw Under Active Exploitation Allows Unauthenticated Code Execution



The Apache Software Foundation reports active exploitation of CVE-2026-129448 (CVSS 9.8) in Apache Roller, a flaw in the XML-RPC endpoint that can lead to remote code execution without authentication.

- Apache Roller is an open-source, Java-based blogging platform.
- The flaw is tracked as CVE-2026-129448 with a CVSS score of 9.8.
- It is an unauthenticated deserialization issue in the XML-RPC endpoint.
- Successful exploitation could lead to remote code execution.
- The Apache Software Foundation says it is being exploited in the wild.

What has been reported

The Apache Software Foundation (ASF) has indicated that a critical vulnerability in Apache Roller is being exploited in the wild. Roller is an open-source blogging platform written in Java.

The flaw is tracked as CVE-2026-129448 and carries a CVSS score of 9.8. It is an unauthenticated deserialization weakness in the XML-RPC endpoint, which could allow an attacker to run code remotely on the affected server.

Why it matters

Because no authentication is required, any exposed Roller instance that reaches the vulnerable endpoint is a potential target. Active exploitation means the window between disclosure and attack is already closed. The source excerpt does not list affected versions or fixed releases, so teams should consult the official ASF advisory for those details.

Recommended approach

Institutions should first establish whether Apache Roller is used anywhere in their estate, including internal knowledge portals, marketing sites or systems run by third parties. Where it is found, exposure of the XML-RPC endpoint should be reduced while the vendor guidance is reviewed and applied.

If an instance has been reachable from the internet, treat it as potentially compromised until review shows otherwise, and preserve logs for investigation.

What to do now

1. Inventory all Apache Roller instances, including those run by vendors or business units.
2. Check the official ASF advisory for affected and fixed versions and apply the update.
3. Restrict or block internet access to the XML-RPC endpoint until patched.
4. Review web and application logs for suspicious XML-RPC requests and preserve them.
5. Treat internet-exposed instances as potentially compromised and start incident triage.
6. Report confirmed incidents through the channels required by your sector regulator.