CVE-2024-51504: Apache ZooKeeper: Authentication bypass with IP-based authentication in Admin Server

Posted to user@zookeeper.apache.org (list.html?user@zookeeper.apache.org)

Andor Molnar - Wednesday, November 6, 2024 11:30:09 PM GMT+8

Severity: important

Affected versions:

- Apache ZooKeeper 3.9.0 before 3.9.3

Description:

When using IPAuthenticationProvider in ZooKeeper Admin Server there is a possibility of Authentication Bypass by Spoofing -- this only impacts IP based authentication implemented in ZooKeeper Admin Server. Default configuration of client's IP address detection in IPAuthenticationProvider, which uses HTTP request headers, is weak and allows an attacker to bypass authentication via spoofing client's IP address in request headers. Default configuration honors X-Forwarded-For HTTP header to read client's IP address. X-Forwarded-For request header is mainly used by proxy servers to identify the client and can be easily spoofed by an attacker pretending that the request comes from a different IP address. Admin Server commands, such as snapshot and restore arbitrarily can be executed on successful exploitation which could potentially lead to information leakage or service availability issues. Users are recommended to upgrade to version 3.9.3, which fixes this issue.

Credit:

4ra1n (reporter)
Y4tacker (reporter)

References:

https://zookeeper.apache.org (https://zookeeper.apache.org)/
https://www.cve.org/CVERecord?id=CVE-2024-51504 (https://www.cve.org/CVERecord?id=CVE-2024-51504)

✎ 🔗 (thr

Andor Molnar - Thursday, November 7, 2024 1:21:37 AM GMT+8

Website updated.