CVE-2023-34468 – Score: 8.8

Components:

apache nifi *

Description:

The DBCPConnectionPool and HikariCPConnectionPool Controller Services in Apache NiFi 0.0.2 through 1.21.0 allow an authenticated and authorized user to configure a Database URL with the H2 driver that enables custom code execution. The resolution validates the Database URL and rejects H2 JDBC locations. You are recommended to upgrade to version 1.22.0 or later which fixes this issue.

Main problems:

94 "Improper Control of Generation of Code ('Code Injection')"