CVE-2023-43651 - Score: 8.5

Components:

fit2cloud jumpserver *

Description:

JumpServer is an open source bastion host. An authenticated user can exploit a vulnerability in MongoDB sessions to execute arbitrary commands, leading to remote code execution. This vulnerability may further be leveraged to gain root privileges on the system. Through the WEB CLI interface provided by the koko component, a user logs into the authorized mongoDB database and exploits the MongoDB session to execute arbitrary commands. This vulnerability has been addressed in versions 2.28.20 and 3.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.

Main problems:

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