CVE-2021-35464 - Score: 9.8

Components:

    forgerock openam *
    forgerock am *

Description:

ForgeRock AM server before 7.0 has a Java deserialization vulnerability in the jato.pageSession parameter on multiple pages. The exploitation does not require authentication, and remote code execution can be triggered by sending a single crafted /ccversion/* request to the server. The vulnerability exists due to the usage of Sun ONE Application Framework (JATO) found in versions of Java 8 or earlier

Main problems:

502 "Deserialization of Untrusted Data"