NVD DB Update

CVE-2024-9053 - Score: 9.8

Components:

Description:

vllm-project vllm version 0.6.0 contains a vulnerability in the AsyncEngineRPCServer() RPC server entrypoints. The core functionality run_server_loop() calls the function _make_handler_coro(), which directly uses cloudpickle.loads() on received messages without any sanitization. This can result in remote code execution by deserializing malicious pickle data.

Main problems:

78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')"

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa