









com/thoughtworks/go/agent/Agent ProcessParentImpl.java	172	2	SECURITY	COMMAND_INJECTION	 
com/thoughtworks/go/util/ command/ProcessRunner.java	37	2	SECURITY	COMMAND_INJECTION	 
com/thoughtworks/go/util/Process Manager.java	48	2	SECURITY	COMMAND_INJECTION	 
com/thoughtworks/go/utis/ CommandUtils.java	45	2	SECURITY	COMMAND_INJECTION	 

```

Process invoke(String[] command) throws IOException {
    ProcessBuilder processBuilder = new ProcessBuilder(command);
    return processBuilder.start();
}

private static class Shutdown extends Thread {
    private static final Logger LOG = LoggerFactory.getLogger(Shutdown.class);
    private final Process agent;

    public Shutdown(Process agent) {
        setName("Shutdown" + getName());
        this.agent = agent;
    }

    @Override
    public void run() {
        LOG.info("Shutdown hook invoked. Shutting down [%s], agent);
        agent.destroy();
    }
}
}
"agent-process-launcher/src/main/java/com/thoughtworks/go/agent/AgentProcessParentImpl.java" 191L, 8517C 172,9

```

```

private ProcessBuilder builder;
private boolean failOnError = true;

public ProcessRunner() {
    builder = new ProcessBuilder();
}

public ProcessRunner command(String... command) {
    builder.command(command);
    return this;
}

public ProcessRunner withWorkingDir(String directory) {
    builder.directory(new File(directory));
    return this;
}

public ProcessRunner failOnError(boolean failOnError) {
    this.failOnError = failOnError;
    return this;
}
}
"util/src/main/java/com/thoughtworks/go/util/command/ProcessRunner.java" 66L, 2423C 37,33

```

```

ConsoleOutputStreamConsumer consumer, ProcessTag processTag, String encoding, String errorPrefix) {
    ProcessBuilder processBuilder = new ProcessBuilder(commandline);
}
"commandline/src/main/java/com/thoughtworks/go/util/ProcessManager.java" 107L, 4242C 48,72

```

```

public static String exec(File workingDirectory, String... commands) {
    try {
        Process process = Runtime.getRuntime().exec(commands, null, workingDirectory);
        return captureOutput(process);
    } catch (Exception e) {
        throw bomb(e);
    }
}
"util/src/main/java/com/thoughtworks/go/utis/CommandUtils.java" 95L, 3723C 45,90

```

This usage of java/lang/ProcessBuilder.command([Ljava/lang/String;)Ljava/lang/ProcessBuilder; can be vulnerable to Command Injection

The highlighted API is used to execute a system command. If unfiltered input is passed to this API, it can lead to arbitrary command execution.

Vulnerable Code:

```
import java.lang.Runtime; Runtime r = Runtime.getRuntime(); r.exec("/bin/sh -c some_tool" + input);
```

References

OWASP: Command Injection

OWASP: Top 10 2013-A1-Injection

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')