# TTP Detail – T1559.003

## TTP Information

Name: XPC Services

Description: Adversaries can provide malicious content to an XPC service daemon for local code execution. macOS uses XPC services for basic inter-process communication between various processes, such as between the XPC Service daemon and third-party application privileged helper tools. Applications can send messages to the XPC Service daemon, which runs as root, using the low-level XPC Service <code>C API</code> or the high level <code>NSXPCConnection API</code> in order to handle tasks that require elevated privileges (such as network connections). Applications are responsible for providing the protocol definition which serves as a blueprint of the XPC services. Developers typically use XPC Services to provide applications stability and privilege separation between the application client and the daemon.(Citation: creatingXPCservices)(Citation: Designing Daemons Apple Dev)

Adversaries can abuse XPC services to execute malicious content. Requests for malicious execution can be passed through the application's XPC Services handler.(Citation: CVMServer Vuln)(Citation: Learn XPC Exploitation) This may also include identifying and abusing improper XPC client validation and/or poor sanitization of input parameters to conduct [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution