Inter-Process Communication: XPC Services, Sub-technique T1559.003 - Enterprise

Archived: 2026-04-02 12:24:14 UTC

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 `C API` or the high level `NSXPCConnection API` 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.[1][2]

Adversaries can abuse XPC services to execute malicious content. Requests for malicious execution can be passed through the application's XPC Services handler.[3][4] This may also include identifying and abusing improper XPC client validation and/or poor sanitization of input parameters to conduct Exploitation for Privilege Escalation.

Source: https://attack.mitre.org/techniques/T1559/003