Detect Abuse of XPC Services (T1559.003), Detection Strategy DET0335

Archived: 2026-04-05 14:05:16 UTC

AN0948

Detects anomalous use of macOS XPC services for code execution. Monitors for processes invoking privileged XPC daemons with abnormal parameters, unexpected binaries communicating over NSXPCConnection, or helper tools executing code outside of their expected parent process lineage. Correlates process access attempts to system-level daemons, privilege escalations via XPC misconfigurations, and injection of malicious payloads through inter-process communication.

Log Sources

Data Component	Name	Channel
Process Access (DC0035)	macos:unifiedlog	Unexpected NSXPCConnection calls by non-Apple-signed or abnormal binaries
Process Creation (DC0032)	macos:unifiedlog	execve: Helper tools invoked through XPC executing unexpected binaries
Named Pipe Metadata (DC0048)	macos:unifiedlog	XPC messages requesting privileged actions from untrusted or unsigned clients

Mutable Elements

Field	Description
AllowedXPCClients	Maintain allowlist of binaries permitted to invoke specific XPC services to minimize false positives.
TimeWindow	Threshold for correlating abnormal XPC requests with subsequent privilege escalation or process creation.
UnsignedBinaryAlertLevel	Adjust sensitivity of alerts for unsigned or non-Apple-signed clients initiating XPC communication.