Detect XSL Script Abuse via msxsl and wmic, Detection Strategy DET0205

Archived: 2026-04-05 16:24:05 UTC

AN0581

Execution of XSL scripts via msxsl.exe or wmic.exe using embedded JScript or VBScript for proxy execution. Detection correlates process creation, command-line patterns, and module load behavior of scripting components (e.g., jscript.dll).

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	May need to tune based on encoded input or custom extensions (e.g., .jpeg instead of .xsl).
ParentProcess	Legitimate administrative or developer tools may use msxsl; validate the parent process chain.
TimeWindow	Temporal correlation window between script engine DLL load and suspicious process spawn.
RemoteXSLDomainWhitelist	Filter known safe URLs used by enterprise for XSL transformations.
