Detection Strategy for Hijack Execution Flow through Services File Permissions Weakness., Detection Strategy DET0436

Archived: 2026-04-05 14:19:12 UTC

Analytics

- Windows

AN1211

Modification or replacement of service executables due to weak file or directory permissions. Defender observes file writes to service binary paths, unexpected modifications of executables associated with registered services, and subsequent service execution of attacker-supplied binaries under elevated permissions.

Log Sources

Mutable Elements

Field	Description
MonitoredServices	List of critical services and their expected executable paths for integrity checking.
HashBaseline	Baseline hashes of legitimate service executables for tamper detection.
TimeWindow	Correlation interval between file modification of service executables and service execution.
PrivilegedAccounts	Accounts allowed to legitimately modify service executables.
