Multi-Platform File and Directory Permissions Modification Detection Strategy, Detection Strategy DET0299

Archived: 2026-04-05 18:14:49 UTC

AN0834

Sequential behavioral chain of privilege escalation through permission modification: (1) Process creation of permission-modifying utilities (icacls, takeown, attrib, cacls), (2) Correlation with unusual user context or timing, (3) DACL modification events targeting sensitive files/directories, (4) Subsequent file access or modification attempts indicating successful privilege bypass

Log Sources

Mutable Elements

Field	Description
TimeWindow	Temporal correlation window for linking permission modification with subsequent access attempts (default: 300 seconds)
SensitivePathList	Environment-specific critical file and directory paths requiring permission change monitoring
TrustedUserContext	Administrative accounts authorized to perform legitimate permission modifications
BusinessHoursThreshold	Time-based threshold for elevated alerting on permission changes outside business hours

AN0835

Behavioral sequence of unauthorized privilege escalation via permission modification: (1) chmod/chown/setfacl process execution with suspicious parameters, (2) Targeting of critical system files or unusual permission values, (3) Correlation with non-privileged user context or unusual timing patterns, (4) Follow-on file access indicating successful permission bypass

Log Sources

Data Component	Name	Channel
File Metadata (DC0059)	auditd:SYSCALL	syscall in (chmod, fchmod, fchmodat, chown, fchown, fchownat, setxattr, lsetxattr, fsetxattr)

Data Component	Name	Channel
Command Execution (DC0064)	auditd:PROCTITLE	proctitle contains chmod, chown, setfacl, or attr commands with suspicious parameters

Mutable Elements

Field	Description
SuspiciousPermissionValues	Octal permission values that indicate potential malicious intent (default: 777, 755, 4755)
CriticalPathPatterns	Linux filesystem paths requiring enhanced monitoring (/etc/, /usr/bin/, /home/)
AuthorizedAdminUsers	User accounts permitted to perform system-level permission modifications
AnomalyThreshold	Statistical threshold for detecting unusual permission modification frequency

AN0836

macOS-specific permission modification behavioral chain: (1) chmod/chown/chflags process execution, (2) System Integrity Protection (SIP) bypass attempts, (3) Extended attribute (xattr) modifications, (4) Unified log correlation with file system events, (5) Subsequent access to previously restricted resources

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	process execution events for chmod, chown, chflags with unusual parameters or targets
File Metadata (DC0059)	fs:fsevents	file system events indicating permission or attribute changes

Mutable Elements

Field	Description
SIPProtectedPaths	macOS system paths protected by SIP that should never have permission modifications
SuspiciousFlagCombinations	chflags parameter combinations indicating evasive behavior (uchg, schg, hidden)
XattrMonitoringScope	Extended attributes to monitor for unauthorized modifications

Field	Description
UnifiedLogRetention	Log retention period for correlating permission changes with subsequent access

AN0837

ESXi hypervisor permission modification behavioral chain: (1) SSH access to ESXi host, (2) chmod/chown execution on VMFS datastore files or system configuration, (3) Modification of VM configuration files (.vmx) or virtual disk permissions, (4) Hostd service log correlation, (5) vCenter permission change events if centrally managed

Log Sources

Mutable Elements

Field	Description
AuthorizedSSHUsers	ESXi user accounts authorized for shell access and file system operations
CriticalVMFSPaths	VMFS datastore paths requiring permission change monitoring
ShellAccessTimeWindow	Time correlation window for linking SSH access with permission modifications
vCenterIntegrationScope	Scope of vCenter audit event correlation with ESXi host activities

---