Detect Malicious Modification of Pluggable Authentication Modules (PAM), Detection Strategy DET0454

Archived: 2026-04-02 12:36:15 UTC

Analytics

- Linux
- macOS

AN1250

Detects unauthorized modifications to PAM configuration files or shared object modules. Correlates file modification events under /etc/pam.d/ or /lib/security/ with unusual authentication activity such as multiple simultaneous logins, off-hours logins, or logons without corresponding physical/VPN access.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	List of PAM configuration and module directories monitored (e.g., /etc/pam.d/, /lib/security/).
TimeWindow	Timeframe for correlating suspicious file modifications with anomalous login events.
BaselineAccounts	Expected login frequency and systems per user account; deviations may indicate compromise.

AN1251

Detects suspicious changes to macOS authorization and PAM plugin files. Correlates file modifications under /etc/pam.d/ or /Library/Security/SecurityAgentPlugins with unexpected authentication attempts or anomalous account usage.

Log Sources

Mutable Elements

Field	Description
WatchedPlugins	Expected set of PAM and authorization plugins; unknown additions may indicate malicious insertion.
CorrelatedSources	Cross-correlation with VPN/physical access logs to identify impossible or anomalous login patterns.

Source: https://attack.mitre.org/detectionstrategies/DET0454#AN1250