Detection Strategy for Weaken Encryption: Reduce Key Space on Network Devices, Detection Strategy DET0243

Archived: 2026-04-05 17:08:15 UTC

AN0681

Defenders may observe attempts to alter cryptographic settings on network devices that reduce key strength or allowable cipher suites. Suspicious indicators include configuration changes that downgrade encryption algorithms, key length parameters, or the disabling of strong encryption in favor of legacy ciphers. These activities often appear as CLI commands modifying crypto policies, firmware changes affecting crypto libraries, or unexpected updates to key management files. Correlation across device config logs and traffic analysis showing weaker ciphers provides higher confidence of malicious key space reduction.

Log Sources

Data Component	Name	Channel
File Modification (DC0061)	networkdevice:config	Configuration changes referencing 'crypto', 'key length', 'cipher', or downgrade of encryption settings
Command Execution (DC0064)	networkdevice:cli	Execution of CLI commands altering crypto parameters (e.g., 'crypto key generate rsa modulus 512')
Network Traffic Content (DC0085)	NSM:Flow	Observed downgrade in negotiated cipher suites or TLS/SSH versions across sessions

Mutable Elements

Field	Description
AllowedKeyLengths	Defines the minimum acceptable encryption key sizes; tunable to organizational policy.
CipherSuiteBaseline	Baseline list of approved cipher suites for network sessions; deviations may indicate tampering.
AuthorizedAdminAccounts	Whitelisted accounts for executing crypto configuration changes; ensures alerts only trigger on unauthorized actions.
TimeWindow	Time correlation period between configuration change and anomalous traffic downgrade; adjustable to reduce noise.
