Detection Strategy for Patch System Image on Network Devices, Detection Strategy DET0469

Archived: 2026-04-05 15:55:19 UTC

AN1293

Defenders may observe adversary attempts to patch system images by monitoring for anomalous file transfers (TFTP, SCP, FTP) of image files, unauthorized CLI commands altering boot system variables, integrity check mismatches between running and baseline OS images, and runtime memory manipulation attempts. Suspicious sequences include uploading a new image, modifying boot parameters, and subsequent reload/reboot of the device. In-memory patching attempts may manifest as debug commands or boot loader manipulation inconsistent with normal administrative activity.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:cli	Execution of privileged commands such as 'copy tftp flash', 'boot system', or 'debug memory'
File Modification (DC0061)	networkdevice:config	Configuration changes to startup image paths, boot loader parameters, or debug flags
Firmware Modification (DC0004)	firmware:runtime	Debug or memory access commands indicating attempts to alter OS instructions in memory

Mutable Elements

Field	Description
ApprovedFirmwareVersions	Whitelist of validated vendor OS versions; deviations may indicate tampering.
AuthorizedAdminAccounts	Trusted admin accounts permitted to update images; anomalies suggest compromise.
ChecksumBaseline	Baseline hash of approved images; used for detecting file tampering.
TimeWindow	Correlation period for detecting chained behaviors (file upload → boot config change → reboot).