Detection Strategy for T1542.001 Pre-OS Boot: System Firmware, Detection Strategy DET0099

Archived: 2026-04-05 13:55:44 UTC

AN0275

Unexpected write operations to BIOS/UEFI firmware regions or EFI boot partitions that do not correlate with legitimate vendor firmware updates. API calls or utilities such as fwupdate.exe or vendor flash tools executed from non-administrative or non-IT management accounts. Suspicious raw disk writes targeting System Firmware GUID partitions followed by abnormal reboot sequences.

Log Sources

Mutable Elements

Field	Description
AllowedFirmwareUpdateTools	Legitimate vendor tools permitted to perform firmware flashing or BIOS updates.
TimeWindow	Expected time periods for approved firmware updates, used for correlating suspicious activity outside patch cycles.
KnownGoodFirmwareHashes	Baseline hashes of vendor BIOS/UEFI firmware for integrity comparison.

AN0276

Unauthorized firmware uploads to routers, switches, or firewalls via TFTP/FTP/SCP. Logs showing boot variable or startup image path changes redirecting to non-standard firmware images. Abnormal reboots or firmware rollback attempts following configuration modification events.

Log Sources

Mutable Elements

Field	Description
ApprovedFirmwareHashes	Known good firmware image hashes stored for validation.
MaintenanceWindows	Expected time periods when firmware uploads or reboots are considered normal.

Field	Description
SourceIPWhitelist	List of trusted management IPs allowed to initiate firmware uploads.

Source: https://attack.mitre.org/detectionstrategies/DET0099#AN0276