Detect Abuse of vSphere Installation Bundles (VIBs) for Persistent Access, Detection Strategy DET0535

Archived: 2026-04-02 11:51:40 UTC

Analytics

- ESXi

AN1475

Malicious VIB installation for persistence via `esxcli software vib install` using `--force` or `--no-sig-check`, enabling custom startup scripts or firewall rules. Behavior chain: (1) unsigned/suspicious VIB installation → (2) startup script or binary placed in persistent boot path → (3) persistence across reboot via /etc/rc.local.d or other boot hook).

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	esxi:esxupdate	/var/log/esxupdate.log contains VIB installed with `--force` or `--no-sig-check` and non-standard acceptance levels
Command Execution (DC0064)	esxi:shell	`esxcli software vib install` with `--force` or `--no-sig-check` from shell history or `shell.log`
File Modification (DC0061)	linux:fim	Changes to /etc/rc.local.d/local.sh or creation of unexpected startup files in persistent partitions (/etc/init.d, /store, /locker)

Mutable Elements

Field	Description
AcceptanceLevel	Some environments may intentionally permit CommunitySupported or unsigned VIBs—filter by known allowed publishers.
InstallCommandThreshold	Set alerting thresholds for frequency of VIB install attempts per host/user/time window.
StartupPathRegex	Tune regex for monitoring startup file locations based on ESXi image customization.

Source: https://attack.mitre.org/detectionstrategies/DET0535#AN1475