MA.L2-3.7.4

Maintenance

Media Inspection

"Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems."

Objectives

[a]

Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

Key Discussion Points

Before Use, Not After:
The scan happens before the media is used on a CUI system — discovering malware after connection is too late.

Any Source, Any Format:
Vendor FTP downloads, email attachments, USB drives, and cloud-shared utilities all require inspection before use on CUI systems.

Extends SI.L2-3.14:
3.7.4 extends SI.L2-3.14.2 and 3.14.4 — the malware protection requirements — specifically to diagnostic and test media.

Hash Verification:
The guide example includes verifying the file hash against vendor-provided values — integrity checking is part of proper media inspection.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan.

INTERVIEW

Personnel with system maintenance responsibilities; personnel with information security responsibilities.

TEST

Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance.

MA.L2-3.7.4

MAINTENANCE — Media Inspection

Plain English

What this control is really saying:

A vendor sends you a diagnostic utility via FTP. You download it, run it, and it installs malware on your CUI server. This control requires one step before that: scan it first. Any media containing diagnostic or test programs must be checked for malicious code before it touches your systems.

How it is used:

- All vendor-provided diagnostic files are scanned with current AV software before being executed on any CUI system — scan results are logged.
- USB drives brought in for maintenance are scanned on an isolated workstation before connecting to CUI systems — no direct connection without a clean scan.
- File hash values are verified against vendor-published checksums when available — discrepancies trigger an immediate stop and an incident report.
- The IT admin documents each media inspection event: source, file name, scan date, scan tool version, and result.

Real World Example

The Scenario

A vendor technician provides a diagnostic utility via an anonymous FTP link to troubleshoot a server issue. The IT admin downloads the file and runs it immediately on the CUI server without scanning it. The utility installs a remote access agent.

What the assessor finds

The remote access agent begins beaconing to an external IP. There is no media inspection procedure and no scan was performed. The incident was discovered during a routine log review two weeks later. The utility came from an unauthenticated FTP source with no hash provided.

SPRS Score Impact

3.7.4 carries a point value of 3. Unscanned diagnostic media is a well-documented supply chain attack vector — attackers compromise vendor tools or FTP repositories to deliver malware through trusted maintenance channels.

What Good Looks Like

Written procedure for media inspection before use, AV signatures current, all vendor-provided files scanned on isolated workstation, hash verification against vendor checksums, inspection results logged, malicious code findings handled per IRP.

Common Gaps

What assessors actually find in the field:

✗ **No scan before use**

Vendor utilities are downloaded and run directly on CUI systems — no AV scan, no hash check, no inspection process at all.

✗ **Outdated scan signatures**

Media is 'scanned' but the AV definitions are months out of date — the scan provides no meaningful protection against recent malware.

✗ **Scan happens after connection**

USB drives are plugged in first, then scanned — the autorun has already executed before the scan completes.

✗ **No hash verification**

Files are scanned for malware but file integrity is never verified — a modified utility with no known signature passes undetected.

✗ **Process not documented**

Staff informally scan files 'when they remember' but no written procedure or log exists to demonstrate consistent compliance.