CM.L2-3.4.9

Configuration Management

User-Installed Software

"Control and monitor user-installed software."

Objectives

[a]
A policy for controlling the installation of software by users is established.

[b]
Installation of software by users is controlled based on the established policy.

[c]
Installation of software by users is monitored.

Key Discussion Points

Policy First:
A written policy defining what users can and cannot install must exist — without it, monitoring and enforcement have no foundation.

No Admin Rights:
The most effective technical control is simply not giving users local admin rights — they cannot install software they lack privilege to install.

Monitoring Required:
This control requires [c] — monitoring. Even with a policy and technical controls, you must verify compliance and detect violations.

Approved App Sources:
Permitted installations include patches and updates — organizations may also designate approved repositories or 'app stores.'

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing user-installed software; configuration management plan; system security plan; system configuration settings; list of rules governing user-installed software; system monitoring records; system audit logs; continuous monitoring strategy.

INTERVIEW

Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes governing user-installed software; mechanisms enforcing rules for governing software installation by users; mechanisms monitoring policy compliance.

CM.L2-3.4.9

CONFIGURATION MANAGEMENT — User-Installed Software

Plain English

What this control is really saying:

Users installing software without oversight is one of the most common ways malware enters a CUI environment. This control requires a written policy on what users can install, technical controls to enforce it, and monitoring to catch violations. The combination of all three is required — policy alone is not enough.

How it is used:

- The acceptable use policy defines that users may not install any software not approved in writing by the IT admin.
- Standard user accounts on all workstations have no local admin rights — software installation requires IT admin credentials.
- Endpoint management software monitors installed software weekly and alerts the IT admin if any unapproved application appears.
- Users who need a new software tool submit a request form — IT evaluates security risk, approves or denies, and installs if approved.

Real World Example

The Scenario

Acme Defense has an acceptable use policy that mentions not installing unauthorized software. However, all five users have local admin rights on their workstations. No monitoring is in place to track what software gets installed.

What the assessor finds

Three workstations have personal Dropbox clients installed — CUI files are visible in the sync folder. One machine has a remote access tool the user installed for 'convenience.' The IT admin had no idea any of this was installed.

SPRS Score Impact

3.4.9 carries a point value of 3. Uncontrolled user software installation is a direct path for malware and unauthorized data exfiltration — the Dropbox finding alone represents a potential CUI spillage event.

What Good Looks Like

Written policy defining permitted and prohibited installations, no local admin rights for standard users, endpoint monitoring detecting unauthorized software, documented approval process for new software requests.

Common Gaps

What assessors actually find in the field:

✗ **No policy exists**

There is no written rule about what users can or cannot install — software installation is entirely uncontrolled.

✗ **Users have local admin rights**

All workstation users are local administrators — any software can be installed without approval or oversight.

✗ **Policy but no enforcement**

A policy exists saying users should not install software, but nothing technically prevents them from doing so.

✗ **No monitoring**

Software may be controlled but nobody checks — unauthorized installs go undetected until something breaks.

✗ **Shadow IT on CUI systems**

Employees have installed personal cloud sync tools on CUI workstations — now CUI is syncing to personal cloud accounts.