CDM Configuration Settings Management (CSM) Capability

Department of Homeland Security
National Cyber Security Division
Federal Network Security
Network & Infrastructure Security

Table of Contents

1 Purpose and Scope

This toolkit outlines and documents issues of relevance to implementing the Configuration Settings Management (CSM) Capability as part of Continuous Diagnostics and Mitigation (CDM). This toolkit provides general information on CSM and implications thereof. Further, this toolkit highlights potential considerations that technical implementers as well as managers may have when understanding how their organization can effectively implement CSM to better manage cybersecurity risk.

Additional considerations, inquiries, and suggestions for revision or addition can be submitted to: cdm.fnr@hq.dhs.gov. This toolkit will be updated as required.

2 THREAT / ATTACKS

1. QUESTION: WHAT TYPES OF ATTACKS ARE WE TRYING TO ADDRESS WITH CSM?

Answer: CSM mitigates attacks that require successful exploitation of default or poor configuration settings to compromise a device or a system.

Attack Description: Attackers attempt to exploit software or hardware with weak or insecure configurations. Once a configuration setting is compromised, it may be used to compromise confidentiality, integrity, and availability of resources or data residing on systems and networks.

Attack Types: For CSM, our interests include but are not limited to the following:

- Exploitation of default accounts and passwords (e.g., initial router password)
- Exploitation of "out-of-the-box" configurations (e.g., TFTP is enabled)
- Exploitation of inadequate software or hardware configuration settings (e.g., user can modify setting)
- Exploitation of configurations designed for usability and not security (e.g., AutoRun is enabled)
- Exploitation of misconfigured privilege settings or permissions on software and hardware (e.g., configuration file is set to world-writable)

Impact: By reducing the number of weak or incorrect settings, we can reduce the attack surface, making it harder for attackers to succeed.

Configurations can exist for software, hardware, or firmware. Configurations on endpoints can include ports, protocols, or available services.

NIST Guidance:
• NIST 800-128 - Guide for Security-Focused Configuration Management of Information Systems: http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
• NIST SP 800-70 - National Checklist Program for IT Products--Guidelines for Checklist Users and Developers: http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

2. QUESTION: HOW ARE THESE ATTACKS DIFFERENT FROM EXPLOITING VULNERABILITIES IN SOFTWARE?

Answer: Attacks against configuration settings exploit functionality in software or hardware, rather than flaws in the software or hardware. While attacks that exploit vulnerabilities in software (managed by Vulnerability Management) deal with bugs in software's source code and method of operation, attacks against configuration settings exploit default or "out-of-the-box" settings, or misconfigurations caused by administrators who incorrectly configure permissions to a resource.

Differentiation: CSM addresses the need to track and manage configuration settings of assets within an organization. While the Manage Software Inventory capability addresses changes that affect specific versions of patches, updates, plug-ins, and new releases, CSM addresses modifications to the software parameters. Vulnerability Management also ties in closely with this capability–unmanaged or unmodified default configurations on hardware and software assets can lead to exploitable vulnerabilities. Attackers can easily take advantage of these targets of opportunity, also known as "low-hanging fruit" in hacker circles.

Not all vulnerable configuration settings are due to "out-of-the-box" settings. During troubleshooting efforts, administrators sometimes change permissions on files or services to ensure the security settings are not interfering with the execution of a program or service. When inadvertently left in place, these configuration changes can leave the modified application open to attack and exploitation.

3. QUESTION: HOW DOES CSM ADDRESS ATTACKS ON POORLY CONFIGURED SYSTEMS?

Answer: Because poorly configured systems provide attackers with easy targets of opportunity due to quick access to elevated privileges or known default settings, a rigorous configuration settings management process and policies can help identify poor and unsecure configuration settings. After quickly identifying poorly configured systems, the organization has a few options for managing this risk:

Primary Methods

- Quickly configure the system to the correct setting.
- Quickly determine the root cause of the misconfiguration.

Preventative Methods

- Develop processes to perform quality assurance checks of configuration settings of new devices added to your inventory.
- Develop processes to prevent unauthorized individuals from making configuration settings changes.
- Develop processes and policies for configuration settings management and control.

Attackers first seek out assets with default configurations, such as the default admin password on a service, for easy access into other systems. It is the easiest way for an attacker to exploit a network.

3 INTEGRATION

4. QUESTION: WHAT CAPABILITIES SUPPORT CONFIGURATION SETTINGS MANAGEMENT?

Answer: Hardware Asset Management (HWAM) and Software Asset Management (SWAM) support CSM by providing a reliable inventory of hardware and software assets to check for known issues.

5. QUESTION: WHAT CAPABILITIES DOES CSM SUPPORT?

Answer: CSM can aid in proper execution of Vulnerability Management. For example, sometimes enabling or disabling configuration settings in file sharing and in services can help mitigate certain vulnerabilities. More supported capabilities will be added as more phases of CDM are rolled out.

6. QUESTION: WHAT OTHER CAPABILITIES PROVIDE "COMPENSATING CONTROLS" TO CSM?

Answer: SWAM can provide compensating controls to CSM. By preventing vulnerabilities using patching, certain configuration settings can be protected from exploitation. Another way SWAM can provide compensating controls to CSM is through whitelisting or blacklisting. By allowing or disallowing certain software to be installed, whitelists and blacklists reduce the risk that a piece of software could be exploited due to poor or incorrect configurations.

4 DESIRED STATE

7. QUESTION: WHAT IS CONSIDERED A CONFIGURATION SETTING?

Answer: A configuration setting is a piece of metadata about software or hardware that determines how it functions. The value can be changed by an administrator (with proper permissions). A configuration setting can take the form of a default password in a SAM file (in the case of the Windows Operating System), a registry key, or a line in a configuration file that is used by a program when executed. A configuration setting can also take the form of privileges (such as file/folder permissions) that must be set by an administrator.

8. QUESTION: WHAT ARE TYPES OF COMMON CONFIGURATION WEAKNESSES?

Answer: The most common types of configuration weaknesses are associated with default settings. Examples include the following:

- Default accounts and passwords (e.g., initial router password)
- "Out-of-the-box" configurations (e.g., TFTP is enabled)
- Inadequate software or hardware configuration settings (e.g., user can modify setting)
- Configurations designed for usability and not security (e.g., AutoRun is enabled)
- Misconfigured privilege settings or permissions on software and hardware (e.g., configuration file is set to world-writable)

Security weaknesses can occur when users and administrators make an unauthorized software or hardware change for testing or to make a task easier. CSM helps quickly identify and remediate these changes and thus limit an adversary's exposed attack surface.

9. QUESTION: WHAT IS THE CSM "DESIRED STATE"?

Answer: The desired state for CSM is for every authorized device to be configured with the authorized configuration settings as required for the role the device has been assigned. (See SWAM for Roles and Profiles.)

Background: The CSM desired state is an enterprise that comprises hardware and software assets with strong and secure configurations. Desired configuration settings are defined and maintained (e.g., ownership is assigned, settings are authorized, frequent maintenance is performed) in checklists and standard configuration operating system images. This desired state includes establishing and maintaining a secure system software image to build and deploy new systems from within the organization. This image should be based on government and industry best practice checklists and security guides, and it should be backed with an established approval process for any deviations from the baseline. Approved organizational system configuration checklists should be established, maintained, and routinely reviewed. Software checklists should be maintained in a machine-readable format to streamline scanning and testing. Hardware checklists should include diagrams to ensure that the configuration process is repeatable and to reduce mistakes. Quality controls should be designed throughout both the software and hardware configuration process to identify any missed or overlooked steps in the checklists.

10. QUESTION: WHAT IS THE "DESIRED STATE" SPECIFICATION FOR CSM?

Answer: The desired state specification is the authorized configurations defined for authorized software and hardware products in your organization.

Background: Every authorized device has a role, and each role requires a baseline configuration. Each organization should have an inventory, by device, documenting the authorized configuration and thus configuration settings for each device in your enterprise. The organization must decide what software must be protected, and which settings to include in CSM.

Bottom Line: The desired state specification contains a complete listing, by device, of all required configuration settings that should exist on each device in the organization's HWAM inventory.

11. QUESTION: WHAT DATA SHOULD BE RECORDED IN DESIRED STATE?

Answer: The minimal configuration settings management data recorded for the desired state should include the following:

Data Item	Justification
Applicable CPE (vendor, product, version, release level) or equivalent	For defining device types, for supply chain management, and to know what CCEs may apply to the device
Approved baseline configuration version for each setting	For tracking version of baseline configurations
CCE configuration to be followed for each setting	For identifying which CCEs to configure the device to
Local D/A settings in addition to baseline configuration settings	For identifying local D/A requirements beyond baseline configuration settings
What is to be configured for each setting (registry, password, privilege, etc.)	For identifying what needs to be checked for compliance
The validation rule to check for each setting	To identify the check to be run on the metadata of the setting
What constitutes compliance for each setting	To document the definition of compliance for the particular setting

12. QUESTION: HOW DOES MY ORGANIZATION DETERMINE ITS CSM DESIRED STATE?

Answer: The CDM Configuration Settings Management Working Group (CSMWG), which is comprised of members from participating Departments and Agencies, will provide the critical configuration settings for software commonly found on Federal networks. These settings provide the baseline for CSM. If your organization is interested in participating in the CSMWG, please email: cdm.fnr@hq.dhs.gov

Each organization can build on this baseline with configuration settings that are operationally relevant to a unique environment. The CSM desired state for each organization should be set through the use of baseline configuration settings for each device role.

Background: Your organization's configuration settings working group (or other group at the organizational level that reviews configuration settings) should determine the desired state by performing a system requirements analysis for each device role required in the enterprise.

The baseline image for each asset should be the least common denominator across your enterprise with modifications approved by your organization's change management process. These baseline settings and images, along with the approved deviations, are your organization's desired state.

The NIST CCE database provides sample baselines for some of the Common Configurations for known hardware and software devices. http://nvd.nist.gov/cce/

Organizations should have configurations for all applications. The CSMWG provides only the most critical configurations for common applications across the government.

13. QUESTION: IS CONFIGURING SETTINGS RECOMMENDED BY THE CDM CSM WORKING GROUP SUFFICIENT?

Answer: The CSMWG focuses on the core and most common application settings across the U.S. Government. In the end, only your organization can determine what is most important to you and your operations. Each organization must identify the applications that have the most impact and how to properly and securely configure them in order to protect critical information and systems. Each organization has a unique risk environment; your organization must determine which configurations apply to its risk environment, and how to implement those configurations.

14. QUESTION: IS RELYING ON BEST PRACTICE CHECKLISTS ACCEPTABLE FOR CSM?

Answer: Yes, but your organization should ensure that any best practices allow for sufficient usability and security for your operational environment.

Background: Federal agencies are at varying levels of maturity in managing their asset configuration settings. Many agencies use established configuration guidelines and checklists from reputable government and industry sources. Reputable best practice checklists have been developed by the National Institute of Standards and Technology, National Security Agency, Defense Information Systems Agency, and Center for Internet Security.

5 ACTUAL STATE

15. QUESTION: WHAT IS "ACTUAL STATE"?

Answer: The actual state is the current configuration settings on all assets across your network. Depending on what tools and capabilities are available, the actual state can be collected during a periodic asset discovery or through automated polling, asset self-reporting, automation, or other means.

CSM actual state should be based only on authorized assets identified for HWAM and SWAM. The D/A needs to establish a policy through CSM that

any piece of software discovered through CSM is then brought into the SWAM.

16. QUESTION: WHAT MAKES UP MY D/A'S "ACTUAL STATE" INVENTORY?

Answer: The actual state inventory for CSM is a listing, by discovered device, with all collected configuration settings from each device in your D/A.

17. QUESTION: WHAT DATA SHOULD BE RECORDED IN ACTUAL STATE?

Answer: The minimal CSM data recorded for the actual state should include the following:

Data Item	Justification
Expected CPE (vendor, product, version, release level) or equivalent for each setting	For defining device types, for supply chain management, and to know what CCEs may apply to the device
Version of the configuration guideline/rule set used for each setting	For documenting the version of the guideline/rule set all comparisons were made against
Date/Time of Data Collection for each setting	For documenting point in time the checks were accomplished
Device settings were collected from for each setting	For identifying the device checked
What must be returned to show current status for each setting	For identifying current status for each setting

The data collected for the actual state must be machine readable to prevent subjectivity by excluding humans who can misinterpret data.

18. QUESTION: HOW DOES MY ORGANIZATION DETERMINE ITS ACTUAL STATE?

Answer: The actual state for asset configuration is determined by discovering the current configuration settings of all assets on the network. The actual state can be discovered by using tools and capabilities that can interrogate an asset and record its current configuration settings or by using manual methods such as a physical review of a device's settings.

The actual configurations of the device and software assets on the network are compared against the authoritative configurations to determine the gap in actual state. This gap between desired state and actual state, or *delta,* identifies vulnerable assets (e.g., misconfigured or improperly configured hardware or software) that require corrective action.

6 FINDING DEFECTS

19. QUESTION: HOW DOES AN ORGANIZATION FIND THE DIFFERENCE BETWEEN DESIRED STATE AND ACTUAL STATE IN CSM?

Answer: Determining the difference between desired state and actual state for CSM is provided by routine checks on end devices and the verification of configuration compliance status. CDM requires that device state information be returned for some failed checks, changing how the current tools and processes perform configuration settings management. The act of collecting the data is still the comparison of what the configuration *should be* against what the configuration *is actually* set to. Configuration checks must be written in machine-readable code to prevent subjectivity, allowing only for pass or fail decisions.

Defect Type	Detection Rule	Response Options
Unapproved setting/fail against policy (out of compliance)	Setting exists in the actual state and is assigned a positive risk score in the desired state.	Change setting or accept risk score.
Non-reporting devices	The device is in the HWAM desired or actual state, but not in the CSM actual state with timely-enough data.	Restore reporting or declare the device missing/uninstalled/retired in HWAM.

20. QUESTION: HOW DOES AN ORGANIZATION MANAGE POOR CONFIGURATIONS?

Answer: Response options are listed in Question 19.

Ultimately, it is up to each organization to implement policies for managing poor configurations. Poor hardware and software configurations must be addressed in a timely manner to reduce extended exposure to exploitation. Risk scores can be assigned to each improper or misconfigured asset configuration setting. Assets with poor configurations can then be grouped locally for summarization and management (e.g., by department or by section). An overall risk score can be assessed against each object container.

7 FIXING DEFECTS

21. QUESTION: WHAT OPTIONS ARE AVAILABLE FOR ADDRESSING THE DIFFERENCE BETWEEN ACTUAL AND DESIRED STATE?

Answer: Once the organization has identified the differences between actual and desired states, it is able to understand the differences and determine the appropriate corrective actions, such as:

Develop more accurate desired state specifications:

- Establishing and maintaining configuration inventories

- Establishing and updating baseline configurations for systems
- Having processes in place to make changes in a controlled and approved fashion

Manage deployed configurations and monitor changes:

- Auditing changes in place against those established in the inventory or baseline
- Having a controlled process for exceptions with periodic review
- Having automated mechanisms to centrally manage, apply, and verify configurations
- Establishing non-persistent settings to protect against unauthorized changes

In addition, the response options listed below may help when defects are found between CSM actual and desired states:

Defect Type	Detection Rule	Response Options
Unapproved setting	Setting exists in the actual state and is assigned a positive risk score in the desired state.	Change setting or accept risk score OR go through change management and approve setting.
Non-reporting devices	The device is in the HWAM desired or actual state, but not in the CSM actual state with sufficiently timely data.	Restore reporting or declare the device missing/uninstalled/retired in HWAM

22. QUESTION: WHY IS THE GAP BETWEEN DESIRED STATE AND ACTUAL STATE IMPORTANT?

Answer: The gap between the desired state and actual state represents the improperly configured assets on the network that are likely to be targeted for exploitation by attackers. Attackers specifically look for and target these machines to gain unauthorized access to the network. Identifying a gap between desired state and actual state also helps the organization understand whether its policies and procedures are functioning correctly (e.g., properly configuring assets on the network or properly changing configurations of assets when standard configurations change).

23. QUESTION: HOW CAN AN ORGANIZATION MINIMIZE EXPOSURE TO POOR CONFIGURATIONS?

Answer: The most effective way to minimize exposure to poor configuration settings is to establish processes and procedures to routinely check, review, and report configuration settings on all assets on the network. Effective options include:

- Establishing and maintaining a secure image
- Establishing and maintaining approved configurations checklists
- Determining actual configurations and comparing them with authoritative approved configurations
- Understanding the delta and determining appropriate corrective actions
- Establishing processes for quickly remediating discovered discrepancies

Attackers often exploit and infiltrate networks through assets whose security configurations have been weakened over time (e.g., configurations in which temporary exceptions were granted for specific short-term business needs but were never removed).