ENTERPRISE SYSTEM MANAGEMENT SECURITY CHECKLIST

Version 1 Release 1.3

10 APRIL 2007

Developed by DISA for the DOD

TABLE OF CONTENTS

1. INTRODUCTION

This document contains procedures that enable qualified personnel to conduct an Enterprise System Management (ESM) Security Readiness Review (SRR). The ESM SRR assesses compliance, in part, with DISA's Recommended Standard Application Security Requirements (Version 1.1 dated May 2006). In order to streamline the SRR process, this Checklist does not cover all of the requirements in that document.

DISA Field Security Operations (FSO) conducts ESM SRRs to provide a minimum level of assurance to DISA, Joint Commands, and other Department of Defense (DOD) organizations that their ESM applications are reasonably secure against attacks that would threaten their mission. The complexity of most mission critical ESM applications precludes a comprehensive security review of all possible security functions and vulnerabilities in the time frame allotted for an ESM System SRR. Nonetheless, the SRR helps organizations address the most common ESM vulnerabilities and identify information assurance (IA) issues that pose an unacceptable risk to operations.

1.1 The Scope of a Review

An ESM Application SRR encompasses the IA control subject areas defined in Department of Defense (DoD) Instruction 8500.2. These subject areas are as follows:

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Continuity
- Vulnerability and Incident Management.

During a full ESM application review, a SRR is performed on each of the components listed above in addition to the ESM application itself. For example, if the application infrastructure consisted of a front-end web server running on Windows and a backend database running on UNIX, then the full review would consist of Web Server, Database, Windows, and UNIX SRRs in addition to the ESM SRR.

If this review is a full system baseline all components will be evaluated. If this review is an ST&E validation or a re-accreditation and current reviews exist for these components, only the vulnerability scan needs to be completed at the time of the ESM review. A current review is defined as a review performed based upon the current STIG. A review is also deemed to not be current if the operating system or component has been reinstalled since the last SRR.

As security is only as strong as its weakest link, a complete security review should involve both the client and server components of the ESM application.

1.2 Pre-Review Activities

This document specifies duties to be completed by a team lead and a reviewer. In some cases, this may be the same person.

To make best use of time on-site, the team lead should perform the following activities prior to arrival, listed in suggested sequence order:

- Work with site to identify personnel to assist the reviewer with the ESM SRR (one or more individuals available to answer the reviewer's questions.
- Determine scope of review (what systems, software and features will or will not be included)
- Obtain an inventory and diagram of all the in-scope components of the ESM infrastructure (OS, database, third-party middleware, libraries and other components), including version information.
- Obtain and review the System Security Authorization Agreement (SSAA), especially its Disaster recovery plans and Diagrams and a description of the environment.
- Obtain a matrix of user types and associated functions within the ESM.
- Obtain dataflow of the ESM functions and network diagrams showing all firewalls and IDS descriptions as well as additional enclave boundaries that the ESM controls.
- Obtain signed SRR coordination memo in which site management accepts the review's scope and the operational risk associated with performing the review.

The reviewer should perform the following activities prior to arrival, listed in suggested sequence order:

- Obtain necessary approvals for physical and logical access to in-scope components. Submit appropriate DD Form 2875s for access to the site.
- Acquire a general knowledge of the ESM, including what it does and the user community it serves.
- Review the matrix of user types and associated functions within the ESM.
- Review dataflow diagram.

- Assist Team Lead in determining the scope of the review.

The term “ESM representative” is used hereafter to denote personnel to assist the reviewer with the ESM SRR. The representative may be an ESM administrator, IAO, Systems administrator or other individual with sufficient knowledge and access to the ESM and ESM applications to permit the reviewer to complete the review. In some cases, the ESM representative role may be split among multiple individuals.

1.3 Recording Results

Once information is gathered and evaluated, the reviewer can record findings of Vulnerabilities in the Checklist SRR Results Report included later in this document.

Results are also entered into the Vulnerability Management System (VMS). Create the asset as a unique entity in the Computing branch and then add the proper targets to the Asset Posture.

1.6 Organization of the Checklist

The remainder of the document is divided into the following sections:

- Section 2 (SRR Report) provides a form on which reviewer will document contacts, the overall components of ESM and the ESM configuration.
- Section 3 (VMS 6.0 ESM Procedures)
- Section 4 (Checklist of all ESM Policy Entries)
- Section 5 (Checklist of all SMS Server Entries)
- Section 6 (Checklist of all SMS Client Entries)

This page is intentionally left blank

2. SRR REPORT

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

2.1 Reviewer Information

Reviewer Name	
Reviewer Phone number	Commercial: DSN:
Reviewer e-mail	
Reviewer SIPRNet e-mail	
ESM STIG version	
ESM Checklist version	
Date of review	
Date of report	

2.2 Site / Organization Information

Organization Name	
Primary Address Street Address City, State ZIP	
IAO Name:	
E-mail Address:	
SIPRNet Address:	
Phone #	Commercial DSN:
ESM System Admin Name:	
ESM System Admin e-mail:	
ESM System Admin SIPRNet e-mail:	
ESM System Admin Phone #	Commercial: DSN:

2.3 ESM Systems Information

Enterprise System Management Name	
MAC Level	☐ I ☐ II ☐ III
Classification	☐ Unclassified ☐ Confidential ☐ Secret ☐ Top Secret

The IAO or information owner should be able to provide the information of the MAC and Classification Level.

Also interview the data owner to determine if sensitive data is being processed by the application.

2.5 ESM Server Overview

List all of the ESM servers and clients regardless of whether they are reviewed or not. If an OS SRR has been or will be performed on that server, place a "Y" in the "Reviewed?" column to the right of the "Operating System and Version" column. Otherwise, enter an "N." For each server, note what ESM software and version is installed (web, database, LDAP, etc.) and whether or not SRRs have been or will be performed on those components.

Host Name	IP Address Subnet Mask	Operating System and Version	Reviewed?	Enterprise System Management Software and Version	Reviewed?	Physical Location

Client Name	IP Address Subnet Mask	Operating System and Version	Reviewed?	Enterprise System Management Software and Version	Reviewed?	Physical Location

Network Information

	Enclave Name	Router	Function	
1				
2				
3				
4				
5				

3. VMS 6.0 ESM Procedures

AS01 Report

The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. In the section "Looking at ESM Assets" is a quick step by step instruction in creating the report.

1. **Look at ESM Assets Non-Computing**
   a. *Steps*
      i. Reports
      ii. AS01
      iii. Select Non-Computing (SUBMIT)
      iv. Select by Location (SUBMIT)
      v. Select the location
         1. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable.
      vi. Expand Non-Computing. - Expand ESM Policy.
      vii. Submit for ESM Asset Report
      viii. View the following website for further details: https://vmscbt.disa.mil/index.htm
   b. *Problems*
      i. The element tree always starts at the top of a page. The element tree only prints for one page. If more data, it is truncated.

2. **Look at ESM Assets Computing**
   a. *Steps*
      i. Reports
      ii. AS01
      iii. Select Computing (SUBMIT)
      iv. Select by Location (SUBMIT)
      v. Select the location
         1. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable.
      vi. Expand Computing. - Expand ESM. – Expand the appropriate ESM Type and check the box next to it.
      vii. Submit for ESM Asset Report
      viii. View the following website for further details: https://vmscbt.disa.mil/index.htm
   b. *Problems*
      i. The element tree always starts at the top of a page. The element tree only prints for one page. If more data, it is truncated.

Performing the Review

If the ESM asset is registered and under the correct location, skip to section titled First Review of the Asset. Ensure that the asset is registered in VMS under the correct organization.

1. **Creating/Registering the Asset Non-Computing**

   a. *Steps*
      i. Expand Asset Findings Maintenance
      ii. Expand Assets/Findings
      iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
      iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
      v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
      vi. Click the yellow folder icon located at the right of 'Non-Computing' to create an Asset. Select the ESM Policy Asset.
      vii. Click the General tab
         - Enter the ESM name in "Display name" and add a Description
         - Note: Use "Managed By" for remote locations being managed.
         - Note: Use "Owner Field" to register asset to parent or child location.
         - Note: Mac level, Confidentiality, & Use are defaulted. Change as required.

      viii. Click the 'Asset Posture' tab to add postures to the asset:
         - Expand Non-Computing
         - Expand ESM Policy
         - Choose the appropriate ESM Type as defined by the ESM STIG – for Non-Computing it will be ESM Policy
         - Click '>>' to move all selected options to the 'Selected' window
         - Click on System/ESM - Determine the ESM that the asset is part of. Enter the ESM on the Systems/ESMs tab of the asset creation / or update screen. For registered ESMs, choose the ESM. If the ESM is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an ESM.
         - Click 'Save'

      Note: When creating a Non-Computing ESM ASSET make sure that the name is unique to the site example (ESM.MECH1.SITE) and not just (ESM)

      View the following website for further details:
      https://vmscbt.disa.mil/index.htm

2. Creating/Registering the Asset Computing

a. Steps

i. Expand Asset Findings Maintenance
ii. Expand Assets/Findings
iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. Click the yellow folder icon located at the right of 'Computing' to create an Asset. Select the ESM Policy Asset.
vii. Click the General tab
- Enter the ESM name in "Display name" and add a Description
- Note: Use "Managed By" for remote locations being managed.
- Note: Use "Owner Field" to register asset to parent or child location.
- Note: Mac level, Confidentiality, & Use are defaulted. Change as required.

viii. Click the 'Asset Posture' tab to add postures to the asset:
- Expand Computing
- Expand ESM
- Choose the appropriate ESM Type as defined by the ESM STIG
- Click '>>' to move all selected options to the 'Selected' window
- Click on System/ESM - Determine the ESM that the asset is part of. Enter the ESM on the Systems/ESMs tab of the asset creation / or update screen. For registered ESMs, choose the ESM. If the ESM is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an ESM.
- Click 'Save'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

3. First Review of the Asset Non-Computing

If the asset is registered and it is the first time it has been reviewed, the following may need to be accomplished.

a. Steps

i. Expand Asset Findings Maintenance
ii. Expand Assets/Findings

iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. Expand 'Non-Computing'.
vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
viii. Click Asset name.
- Verify data in General tab and Asset Posture
- Click the 'Asset Posture' tab to add functions to the asset:
- Expand 'Non-Computing' in the 'Available' window
- Expand 'ESM' in the 'Available' window
- Click the box associated with the correct ESM Type
- Expand the asset in the 'Selected' window
- Click '>>' to move all selected options to the 'Selected' window
- Click on System/ESM - Determine the ESM that the asset is part of. Enter the ESM on the Systems/ESMs tab of the asset creation / or update screen. For registered ESMs, choose the ESM. If the ESM is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an ESM.
- Click 'Save'

ix. Continue with the following section 'Procedures for Review of the Asset' - Must Review'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

4. First Review of the Asset Computing

If the asset is registered and it is the first time it has been reviewed, the following may need to be accomplished.

a. Steps

i. Expand Asset Findings Maintenance
ii. Expand Assets/Findings
iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. Expand 'Computing'.
vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
viii. Click Asset name.

- Verify data in General tab and Asset Posture
- Click the 'Asset Posture' tab to add functions to the asset:
- Expand 'Computing' in the 'Available' window
- Expand 'ESM' in the 'Available' window
- Click the box associated with the correct ESM Type
- Expand the asset in the 'Selected' window
- Click '>>' to move all selected options to the 'Selected' window
- Click on System/ESM - Determine the ESM that the asset is part of. Enter the ESM on the Systems/ESMs tab of the asset creation / or update screen. For registered ESMs, choose the ESM. If the ESM is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an ESM.
- Click 'Save'

ix. Continue with the following section 'Procedures for Review of the Asset' - Must Review'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

5. Procedures for Review of the Asset Non-Computing

If all registration tasks have been accomplished, use the following procedures:

a. Steps

i. Expand Asset Findings Maintenance
ii. Expand Assets/Findings
iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location.*
iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. Expand 'Non-Computing'.
vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
viii. Expand Asset to Review - When you drill down into the asset you will find Vulnerabilities assigned to the ESM Policy component.
ix. Expand a vulnerability
x. Update the 'Status' of the vulnerability
xi. Identify details on all open vulnerabilities
xii. If applicable: Apply to other assets by using the 'apply to other Findings' pane.

Note: Descriptions for Icons and Colors can be obtained in the VMS 6.0 WBT.
https://vmscbt.disa.mil/index.htm

6. Procedures for Review of the Asset Computing

If all registration tasks have been accomplished, use the following procedures:

a. *Steps*
   i. Expand Asset Findings Maintenance
   ii. Expand Assets/Findings
   iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location.*
   iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
   v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
   vi. Expand 'Computing'.
   vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review'.*
   viii. Expand Asset to Review - When you drill down into the asset you will find Vulnerabilities assigned to the ESM component.
   ix. Expand a vulnerability
   x. Update the 'Status' of the vulnerability
   xi. Identify details on all open vulnerabilities
   xii. If applicable: Apply to other assets by using the 'apply to other Findings' pane.

   Note: Descriptions for Icons and Colors can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

7. Verify that all necessary assets were reviewed

a. *Steps*
   i. Asset Findings Maintenance
   ii. Visits
   iii. Expand visit
   iv. Expand location
   v. Expand computing, non-computing, CNDS as applicable.
   vi. Expand 'Must Review'
      1. If checkmarks are gone, the asset has been reviewed or at a minimum has been opened and something has been changed on the asset.

   ii. Reports
      1. VC06 - Asset Compliance Report
      2. Can select an asset or an org.
      3. Select "open" status
      4. Can sort on different fields
      5. Display
         a. Finding Comments
         b. Finding Long Name
            i. Because it is truncated otherwise
         c. Finding Details
         d. Vulnerability Discussion

6. VC03 Severity Summary Report
    a. Has numbers only

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

8. Add Comments

a. Steps

i. Visit Maintenance
ii. Expand Organization the visit is set up for.
iii. Expand Visit
iv. Locate the visit you are working on.
v. Click on CCSD or ESM name.
vi. Comments Tab
vii. Save Changes

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

9. Compliance Monitoring

b. Steps

i. Reports
ii. VC06
iii. Can select an asset or an org.
iv. Select “open” status
v. Can sort on different fields
vi. Display
    1. Finding Comments
    2. Finding Long Name
        a. Because it’s truncated otherwise
    3. Finding Details
    4. Vulnerability Discussion
vii. VC03
    1. Has numbers only

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

4. CHECKLIST INSTRUCTIONS – ESM Policy Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the ESM Policy Checks that must be reviewed regardless of the ESM environment.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

EGA.0040 V0008397 CAT II Unauthorized use of software

8500.2 IA Control: DCPD-1

References: Enterprise System Management STIG Section 3.2.1

Vulnerability Unauthorized use of software

Vulnerability Discussion Public domain software is shareware and there is not any assurance of the products integrity or that security mechanisms exist without a code review or vulnerability analysis. Failure to properly authorize shareware before it is installed or used on corporate AISs could result in compromise of sensitive corporate resources.

Checks **EGA.0040**

The IAO should be interviewed as to the knowledge of any public or freeware software having been installed on the system, and if installed, will provide documented DAA approval.

Default Finding Details The following issues were noted:
Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware is being used without the approval or acknowledgement of the DAA.
The organization is not in compliance with software licensing agreements
The organization is not in compliance with software usage restrictions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0040**

The IAO will ensure that the acquisition of IA or IA-enabled products meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2. If not followed the IAO will provide a statement indicating (1) The software is necessary for mission accomplishment and there are no alternative IT solutions available. (2) The software is assessed for information assurance impacts and approved for use by the DAA.

Notes:

EGA.0050 V0004138 CAT III DOD policy on mobile code is not being followed.

8500.2 IA Control: DCMC-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability DOD policy on mobile code is not being followed.

Vulnerability Discussion Mobile Code is the term given to software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system. An example would be a workstation or laptop, where the recipient executes the web browser without manual installation or initiation of execution by the recipient. Mobile code, such as JavaScript and ActiveX, is particularly vulnerable to malicious attacks. Mobile code is a powerful tool used by developers to run mini applications or scripts, and they are somewhat easily altered.

DoD Directive 8500.1 and the DoD Policy Guidance for use of Mobile Code Technologies require actions to control the threat from mobile code technologies. The DODI 8550.cc, Use of Mobile Code Technologies in DOD Information Systems, provides usage guidance on mobile code.

Checks **EN710**

Interview the IAO to ensure familiarity with DOD Mobile Code policy and implementation.

Determine moblie code compliance with results obtained from Application, Web, and Desktop reviewers.
Mobile Code Policy Follows:
Each browser has various parameters and combinations of parameters that can enforce the DOD Mobile Code Policy Desk Top STIG.
• (DTBG012: CAT I1) The SA will ensure that the browser is configured to disallow unsigned Category I mobile code.
• (DTBG013: CAT I1) The SA will ensure that the browser is configured to only allow signed Category I Mobile Code that has been signed from a trusted source.
• (DTBG014: CAT I1) The SA will ensure that the browser is configured to prompt for execution of signed Category 1 mobile code.
• (DTBG015: CAT I1) The SA will ensure that prohibited CAT 1 mobile code is uninstalled or disabled.
• (DTBG016: CAT I1) The SA will ensure that the browser is configured to only allow Category II mobile code that is signed or received over a trusted channel.

Mobile Code Policy APPLICATION STG

(N/A: CAT I) The ASA will ensure mobile code delivered by the application server is signed with a DOD-approved PKI code-signing certificate or it meets the requirements for use of unsigned code.

Default Finding Details DOD policy on Mobile Code was not followed

---

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EN710**

The IAO will ensure the DODI 8550.cc, Use of Mobile Code Technologies in DOD Information Systems, is adhered to.

Notes:

EGA.0060 V0004017 CAT II Privileged level remote access is not encrypted.

8500.2 IA Control: EBRP-1, EBRU-1

References: Enterprise System Management STIG Section 3.2.2

Vulnerability Privileged level user remote access is not encrypted.

Vulnerability Discussion An attacker can simply wait for authentication of the remote user and then take over or hijack the session and assume the identity of an authorized user. Once the attacker has breached the private network as an authorized mobile user, an attack against strategic network components can be launched.

Checks **EGD.0020**

Interview the IAO and ESM SA to determine that a policy is in place to prohibit privileged level access without encryption. ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption (FIPS 140-2 validated}.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGD.0020**

The IAO will ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption (FIPS 140-2 validated or Type 1), to secure the data traversing the network.

EBRP-1: Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.

Notes:

EGA.0070 V0008399 CAT III Inadequate Configuration Management (CM) process

8500.2 IA Control: DCPR-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability Inadequate Configuration Management (CM) process

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by rigid processes administered by an independent board it much less likely to be in its approved and accredited state.

Checks **EGA.0070**

If this is not a production system, then this check is NA. Interview the IAO to ask if configuration management procedures are in place to prevent untested and uncontrolled software modifications to the production system. If none are in place, then this is a Finding. Sample questions: What procedures do you follow to introduce new software to the production system? Are the modifications tested prior to installation on the production system?

Default Finding Details The following CM issues were noted:
There is no formal Configuration Management Process
The CM process does not include formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
The CM process does not include a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems
The CM process does not include a testing process to verify proposed configuration changes prior to implementation in the operational environment
The CM process does not include a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted

The organization does not employ automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0070**

Develop and implement configuration management procedures for all ESM software modifications and updates.

Notes:

EGA.0080 V0008409 CAT III Inadequate Baseline Software Inventory

8500.2 IA Control: DCSW-1

References: Enterprise System Management STIG Section 3.2.2

Vulnerability Inadequate Baseline Software Inventory

Vulnerability Discussion Rigid control of the system baseline is required if the system is to have any assurance of Information Systems Security. New vulnerabilities are discovered continuously in commercial systems. Care must be taken to track all versions of all commercial products in use so that these deficiencies can be fixed quickly since they are almost immediately the subject of attempted exploits.

Checks **EGA.0080**

Interview the IAO to determine if procedures are in place to baseline and compare stored applications. If they are not, then this is a Finding.

Default Finding Details The following issues were noted:
A baseline software inventory does not exist
The baseline software inventory does not contain all required information
The baseline software inventory does not list all software
The baseline software inventory is not current
Backup copies of software inventory list are not stored off-site or in a fire-rated container.
MAC 1 2 and all classified - The organization does not update the baseline configuration as an integral part of information system component installations.
MAC 1 - The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0080**

Establish and implement inventory management procedures for ESM Software products

Notes:

EGA.0110 V0012056 CAT II The ESM version will soon expire and become unsupp

8500.2 IA Control: DCSL-1

References: Enterprise System Management STIG Section 3.2.2

Vulnerability The ESM version will soon be unsupported and no plan exists to upgrade to a supported version.

Vulnerability Discussion Vendors do not provide security fixes or software updates to unsupported software versions. Unpatched software allows known vulnerabilities to be exploited.

Checks **EGA.0110**

Have SA verify with vendor the dates of new releases of the ESM software, the dates support will be dropped on the current running version, and any patches that have not been installed.

Default Finding Details The following ESM products will expire in the next few months:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0110**

Have the SA establish procedures to record the version numbers of ESM software every month, log status of current and future versions, when support will be dropped on the current version, and verify if any patches have been developed that have not been installed.

Notes:

EGA.0130 V0008395 CAT III User interface services not separated

8500.2 IA Control: DCPA-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability User interface services not separated from data storage and management services.

Vulnerability Discussion Seperation of interface services creates further restrictions of access to the platform on which the data resides and protects the integrity of the system and data.

Checks **EGA.0130**

Review the application architecture identify the application's interface and verify that it is separated from its data base and management services.

Default Finding Details User interface services are not physically or logically separated from data storage and management services.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0130**

Have the SA verify that ESM components such as DBMS be installed on a host system dedicated to its support. By separating the DBMS server, access to that platform can be more finely controlled, resulting in reduced exposure to vulnerabilities in the DBMS software

Notes:

EGA.0140 V0008402 CAT II The security support structure is not isolated

8500.2 IA Control: DCSP-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability The security support structure is not isolated. Security devices such as audit servers, IA tools management consoles and firewall controls are not located in a separate addressable domain. Insure these types of devices are in a separate domain protected/isolated from any other production or user based traffic.

Vulnerability Discussion Keeping Security isolated fom other production or user based traffic, protects it from unathorized access and protects the integity of the system.

Checks **EGA.0140**

Verify that ESM products that provide specific IA functions, such as those that perform provisioning of user identities or enterprise resource access control, are isolated from production or user based traffic. This separation allows control of access to, and integrity of, the hardware, software, and firmware used for securing the system.

Default Finding Details The following issues were noted:
Security devices such as audit servers, IA tools management consoles and firewall controls are not located in a separate addressable domain. Insure these types of devices are in a separate domain protected/isolated from any other production or user based traffic.
For Lab tested IA tools ensure this requirement is addressed in the PMs deployment plan.

Insure that security devices execute dedicated services. For example, a firewall should not run DNS or a Domain Controller should not run a user accessible web server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGA.0140**

The SA will ensure that ESM components that perform I A security functions, including but not limited to user account administration and resource access control, are isolated from production or user based traffic, to separate partitions or domains.

Notes:

EGB.0010 V0008468 CAT II Inadequate Individual I & A

8500.2 IA Control: IAIA-1 References: Enterprise System Management STIG Section 3.3.1

Vulnerability Inadequate Individual Identification and Authentication, or passwords are stored in code or scripts.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **EGB.0010**

Work with the IAO and ESM Admin. to determine compliance to the following criteria is met;
A two-factor authentication system (e.g., a unique token or user logon ID and password) is was used.

EGB.0050

Verify with the IAO that passwords meet the following criteria:
- Passwords are at least eight characters long.
- Passwords are composed of a case sensitive mix including at least one upper case letter, lower case letter, number, and special character.
- Passwords are not the same as the associated ID.
- At least four characters are changed when a new password is created.
- Passwords cannot be changed more than once in any 24- hour period without the intervention of the IAO.
- Passwords expire automatically at least every 90 days.
- The last 10 passwords are not reused.

EGC.0080

Interview the IAO to determine if there is a process or procedure in place to determine a demonstrated need-to-know for access to DOD information. The process or policy must ensure that discretionary or role-based access controls are established and enforced, via operating system controls and access authorization forms, by the Information Owner. The IAO/IAM must enforce the establishment and use of RBAC and discretionary access controls

EGB.0090

Check product installs to see if any factory set passwords are being used. Try to access the product using the factory set password.

Default Finding Details One or more of the following items were found:
A two-factor authentication system (e.g., a unique token or user logon ID and password) is not used.
Related to password:
password used is not a case sensitive, 8- character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.
at least 4 characters are not required to be changed when a new password is created.
registration to receive a user ID and password does not include authorization by a supervisor
the request for a new password is not done in person before a designated registration authority
system mechanisms do not enforce automatic expiration of passwords
system mechanisms do not prevent password reuse
processes are not in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a users password
factory set, default or standard-user IDs and passwords were not removed or changed
authenticators are not protected commensurate with the classification or sensitivity of the information accessed
passwords or other authenticators are shared
passwords are not encrypted for storage
Passwords are not encrypted for transmission
passwords or other authenticators are embedded in access scripts or stored on function keys

MAC 1 and Classified
The information system does not employ multifactor authentication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGB.0010**

The IAO will ensure all user ids and passwords meet DODI 8500.2 IA Implementation Policy.

Notes:

EGB.0020 V0008473 CAT III Improper IA method in use

8500.2 IA Control: IATS-2 References: Enterprise System Management STIG Section 3.3.1

Vulnerability Improper IA method in use

Vulnerability Discussion Due to the capabilities of ESM software to control and modify multiple environments. It is important to have it secured with DoD PKI Class 3 hardware security token.

Checks EGB.0020

Validate the applicaion is pK-enabled, determine what components of the application are PK-enabled (most likely authentication) and work with the IAO and application SA to validate that That the app only used DoD certs .

Default Finding Details Identification and Authentication to all systems is not accomplished using the DoD PKI Class 3 and hardware security token.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0020

Have IAO make sure that PKI technologies used are compatible with the DoD PKI.

Notes:

EGB.0030 V0008467 CAT II Unapproved group authenticators in use

8500.2 IA Control: IAGA-1 References: Enterprise System Management STIG Section 3.3.1

Vulnerability Unapproved group authenticators in use for shared accounts.

Vulnerability Discussion Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has to be explicitly approved by the Designated Approving Authority (DAA). Having group accounts does not allow for proper auditing of who is accessing or changing the network unless an individual authenticator is also used.

Checks EGB.0030

Validate with the IAO that any group authenticators used are only used in conjunction with an individual authenticator. Have the IAO display that the individual authenticator is defined.

Default Finding Details The following issues were noted:
Group authenticators are used for access without a tie to an individual authenticator.
Group authenticators not based on the DoD PKI has not been explicitly approved by the Designated Approving Authority (DAA).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0030

Require minimum usage of group authenticators and when used make certain that individual authenticator are used.

Notes:

EGB.0100 V0008471 CAT IV Insufficient Key management

8500.2 IA Control: IAKM-3

References: Enterprise System Management STIG Section 3.3.2

Vulnerability Insufficient Key management

Vulnerability Discussion

Checks EGB.0100

Have the IAO and ESM SA verify that Secure key management for ESM applications is achieved by conforming to the policies and procedures implemented through the NSA-managed DoD KMI. This currently includes symmetric key management provided by EKMS and asymmetric key management provided by the DoD PKI.

Default Finding Details Symmetric and asymmetric keys are produced, controlled and distributed using other than NSA-approved key management technology and processes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0100

Verify that all ESM products are NIST approved and follow the guidance of the FIPS 140-2 or FIPS 180-2 directives.

Notes:

EGB.0110 V0008470 CAT III Insufficient Key management

8500.2 IA Control: IAKM-2

References: Enterprise System Management STIG Section 3.3.2

Vulnerability Insufficient Key management, Asymmetric Keys are produced, controlled, and distributed using other than DoD PKI Class 3 or Class 4 certificates

Insufficient Key management of ESM application utilizing symmetric or asymmetric keys on a system processing classified information.

Vulnerability Discussion

Checks **EGB.0110**

Verify with the IAO and SA that all asymmetric key management technology is NSA-approved and that all asymmetric keys are produced, controlled, and
distributed using DOD PKI Class 3 or Class 4 certificates.
Verify that hardware security tokens are used to protect the user's private key (e.g., Common Access Card).

EGB.0120

Verify with the IAO and ESM SA that ESM applications containing classified information are using symmetric or asymmetric keys utilizing NSA-approved key management technology and processes.

Default Finding Details The following issues were noted:
Asymmetric Keys are produced, controlled, and distributed using other than DoD PKI Class 3 or Class 4 certificates and hardware
Hardware security tokens are not used to protect the users private key (e.g., Common Access Card).

Cryptographic solutions should be NSA or NIST approved and follow the guidance of the FIPS 140-2 or FIPS 180-2 directives. Due to the complexity of developing cryptographic algorithms, using custom or nonstandard algorithms may allow an attacker to compromise the intended data security and sensitivity

---

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGB.0110**

Implement and enforce procedures to ensure all asymmetric keys are produced, controlled, and distributed using DOD PKI Class 3 or Class 4 certificates.
Implement and enforce procedures to ensure that hardware security tokens are used to protect the user's private key (e.g.,Common Access Card).

EGB.0120

IAM will validate that ESM applications accessing classified systems will use NSA-approved key management technology and processes

Notes:

EGC.0020 V0008421 CAT II Inadequate audit record content

8500.2 IA Control: ECAR-2

References: Enterprise System Management STIG Section 3.4.1

Vulnerability Inadequate audit record content

Vulnerability Discussion Minimum Audit record content is required to insure detection, attribution and recovery from changes to DOD Information and systems.

Checks **EGC.0020**

Verify with the IAO that updates and changes made to ESM data is being logged to the log data sets being used by the ESM.

Default Finding Details The following required data was missing from audit records:
User ID.
Successful and unsuccessful attempts to access security files
Date and time of the event
Type of event.
Success or failure of event.
Successful and unsuccessful logons.
Denial of access resulting from excessive number of logon attempts.
Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
Activities that might modify, bypass, or negate safeguards controlled by the system (system administrator logon, logging directly onto a router vs. using TACACS+, altering access control lists, or altering security files).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0020**

Review with the IAO the logs and information contained in the logs that he is reviewing weekly. Verify that the records contain the following data: User ID. Successful and unsuccessful attempts to access security files Date and time of the event Type of event. Success or failure of event. Successful and unsuccessful logons. Denial of access resulting from excessive number of logon attempts.

Notes:

EGC.0030 V0008431 CAT II Inadequate encryption of transmitted data

8500.2 IA Control: ECCT-1

References: Enterprise System Management STIG Section 3.4.1

Vulnerability Inadequate encryption of transmitted data

Vulnerability Discussion Failure to encrypt sensitive information during transmission may result in compromise of the information

Checks **EGC.0030**

The ESM Administrator will verify that the cryptographic modules are FIPS-140 compliant using the National Institute of Standards and Technology's FIPS 140-1 and FIPS 140-2.

Default Finding Details The following issues were noted:
Unclassified, sensitive data transmitted through a commercial or wireless network are not encrypted
Unclassified, sensitive data transmitted through a commercial or wireless network are not encrypted using NIST-certified cryptograph

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0030**

The ESM administrator will ensure classified information is not transmitted over any communications system unless it is transmitted using approved NSA security devices in addition to approved security procedures and practices.

Notes:

EGC.0040 V0008432 CAT I Inadequate encryption of transmitted data

8500.2 IA Control: ECCT-2 References: Enterprise System Management STIG Section 3.4.1

Vulnerability Inadequate encryption of transmitted data

Vulnerability Discussion Failure to encrypt sensitive information during transmission may result in compromise of the information

Checks **EGC.0040**

Interview the ESM Administrator and determine if there is a Classified or Sensitive Handling transmitting policy in place to include transmission of ESM data over a network cleared to a lower level .

Default Finding Details The following issues were noted:
Classified data is transmitted through a network that is cleared to a lower level than the data being transmitted is not separately encrypted
Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are not separately encrypted using NSA-approved cryptography

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0040**

The ESM Aministrator will ensure classified information is not transmitted over any communications system unless it is transmitted using approved NSA security devices in addition to approved security procedures and practices.

Notes:

EGC.0050 V0008440 CAT II Separation of duties and least privilege principle

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section 3.4.2

Vulnerability Separation of duties and least privilege principles not enforced

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts.

Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges.

The rules of least privilege and separation of duties must always be enforced.

Checks **EGC.0050**

Interview the IAO to determine if documentation/policy exists to enforce least privilege and need to know principles. Verify that privileged users have separate accounts for privileged functions and non-privileged functions. Ensure that they not using their privileged account for non-privileged functions.

Default Finding Details The following issues were noted:
The principle of least privilege is not being rigorously applied.
The principle of separation of duties is not being enforced.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0050**

The IAM will ensure that privileged users and IAOs only access data, control information, software, and hardware for which they are authorized and have a need-to-know.

Notes:

EGC.0080 V0008448 CAT II Roles-base-access is not used

8500.2 IA Control: ECPA-1

References: Enterprise System Management STIG Section 3.4.2

Vulnerability Roles-base-access is not used

Vulnerability Discussion

Checks EGC.0080

Interview the IAO to determine if there is a process or procedure in place to determine a demonstrated need-to-know for access to DOD information. The process or policy must ensure that discretionary or role-based access controls are established and enforced, via operating system controls and access authorization forms, by the Information Owner. The IAO/IAM must enforce the establishment and use of RBAC and discretionary access controls

Default Finding Details The following Issues were noted:
System management privileges are not broken into roles or security groups
Individuals are not properly assigned to roles or security groups

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0080

IAM/IAO will ensure users have a validated or demonstrated need-to-know to access information, and discretionary or role-based access controls will be established and enforced, via operating system controls and access authorization forms, by the Information Owner.

Notes:

EGC.0090 V0008505 CAT II Improper Access granted

8500.2 IA Control: PRNK-1

References: Enterprise System Management STIG SECTION 3.4.2

Vulnerability Improper Access granted

Vulnerability Discussion Failure to verify clearance, need-to-know, and execute a non-disclosure agreement before granting access to classified or sensitive material can result in compromise or theft of information.

Checks EGC.0090

Work with the traditional reviewer to determine compliance and interview the IAO to determine if there is a policy in place to require system access forms for all users.

Default Finding Details The following issues were noted:
Personnel who are granted access to information do not have a valid Need-to-Know
Personnel who are granted access to information do not have proper security clearance
Personnel who are granted access to information have not executed a Non-Disclosure Agreement.
User registration forms are not maintained/required.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0090

The IAM/IAO will ensure all individuals with access to a DOD system or network require the following in the form of a DD Form 2875 or similar access authentication form: - Verification of the users security clearance and/or investigative requirement for holding an IT (formerly ADP) position. - Verification of the need-to-know and permission to access the data by the information owner. - Verification of training. - Acknowledgment, in writing, of users responsibilities to protect the system, data, and password.

Notes:

EGC.0100 V0008466 CAT II No comprehensive account management process exists

8500.2 IA Control: IAAC-1

References: Enterprise System Management STIG Section 3.4.2

Vulnerability No comprehensive account management process exists

Vulnerability Discussion A comprehensive account management process will ensure that only authorized users can gain access to workstations, applications, and networks and that
individual accounts designated as inactive, suspended, or terminated are promptly deactivated. Such a process greatly reduces the risk that accounts will be misused or hijacked.

Checks **EGC.0100**

Interview the IAO to make sure that ESM accounts includes manual or automated procedures to enforce inactive, suspended, and terminated accounts

Default Finding Details The following issues were noted:
A comprehensive account management process is not implemented to ensure that only authorized users can gain access to workstations, applications, and networks
Individual accounts designated as inactive, suspended, or terminated are not promptly deactivated.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0100**

The IAO/IAM will enforce DOD 8500.2 IAAC-1 on all ESM accounts.

Notes:

EGC.0130 V0008453 CAT II Audit records not properly retained

8500.2 IA Control: ECRR-1

References: Enterprise System Management STIG Section 3.4.4

Vulnerability Audit records not properly retained

Vulnerability Discussion

Checks **EGC.0130**

Interview the IAO and determine that procedures and policies are in place to retain backups of ESM audit data for at least a year.

Default Finding Details Audit records are not being properly retained

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0130**

Have the IAO establish procedures to retain backups of audit records for at least a year.

Notes:

EGC.0140 V0008423 CAT II Inadequate audit record review

8500.2 IA Control: ECAT-1

References: Enterprise System Management STIG Section 3.4.4

Vulnerability Inadequate audit record review and backup.

Vulnerability Discussion Audit records for all sources must be regularly reviewed and suspected violations of IA Policies must be analyzed and reported. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks **EGC.0140**

Verify that the ESM administrator has deployed tools that provide audit data review and reporting capabilities.

EGC.0160

Verify with the IAO that ESM audit data is reviewed weekly and that any IA policy violations are analyzed and reported

Default Finding Details The following issues were noted:
Audit trail records from all available sources are not regularly reviewed for indications of inappropriate or unusual activity.
Suspected violations of IA policies are not analyzed
Suspected violations of IA Policies are not reported in accordance with DoD information system IA procedures.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0140**

Validate with the ESM administrator that tools for reviewing and reporting audit data are available and are being used.

EGC.0160

Have the IAO establish and maintain a log indicating that he has checked ESM Audit data weekly

Notes:

EGC.0150 V0008424 CAT II Inadequate audit record review

8500.2 IA Control: ECAT-2 References: Enterprise System Management STIG Section 3.4.4

Vulnerability Inadequate audit record review

Vulnerability Discussion Audit records for all sources are regularly reviewed and suspected violations of IA Policies must be analyzed and reported. For critical and classified systems, an automated, continuous on-line monitoring and audit trail creation capability must be deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks EGC.0150

Verify with the ESM administrator that an automated procedures if available is in place to ensure on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications and with a user configurable capability to automatically disable the application if serious IA violations are detected

Default Finding Details The following issues were noted:
Audit trail records from all available sources are not regularly reviewed for indications of inappropriate or unusual activity.
Suspected violations of IA policies are not analyzed
Suspected violations of IA Policies are not reported in accordance with DoD information system IA procedures.
There is no automated, continuous on-line monitoring and audit trail creation capability
The automated audit feature does not have the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications
There is no user configurable capability to automatically disable the system if serious IA violations are detected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0150

Have the ESM administrator and the IAO develop a plan to create or purchase an automated system that ensures on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications and with a user configurable capability to automatically disable the application if serious IA violations are detected.

Notes:

EGC.0170 V0008358 CAT II Data backup is not performed at least weekly.

8500.2 IA Control: CODB-1 References: Enterprise System Management STIG Section 3.4.4

Vulnerability Data backup is not performed at least weekly.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover.

Checks EGC.0170

Check with the IAO to determine that ESM audit data was being backed up weekly and is stored offsite for Disaster recovery purposes.

Default Finding Details Data backup is not performed at least weekly.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0170

Have the IAO maintain a list of weekly data backups and verify that ESM audit data is included. Review the Site disaster recovery plan to see that backups are stored offsite.

Notes:

EGC.0180 V0008461 CAT III Excessive access to audit trails

8500.2 IA Control: ECTP-1

References: Enterprise System Management STIG Section 3.4.4

Vulnerability Excessive access to audit trails

Vulnerability Discussion Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

Checks **EGC.0180**

Verify with the IAO that all ESM audit backup data is limited to ESM application processes, ESM administrators and validated users.

Default Finding Details The contents of audit trails are not protected against unauthorized access, modification or deletion.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0180**

The IAO will keep a list of all authorized users of ESM audit data.

Notes:

EGC.0190 V0008438 CAT II Successive logon attempts are not controlled

8500.2 IA Control: ECLO-1

References: Enterprise System Management STIG Section 3.4.5

Vulnerability Successive logon attempts are not controlled

Vulnerability Discussion Attempted logons must be controlled to hamper password guessing exploits.

Concurrent sessions per individual must be controlled to limit denial of service attacks.

Checks **EGC.0190**

Have the ESM administrator demonstrate that successive logon attempts are controlled by attempting to logon wrong.

Default Finding Details The following issues were noted:
Successive logon attempts are not controlled

The number of concurrent sessions allowed per user is not controlled.

NIST AC-10 - The information system limits the number of concurrent sessions for any user.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0190**

Have the ESM administrator control Successive logon attempts

Notes:

EGC.0200 V0008439 CAT II Logon attempts & Sessions not limited

8500.2 IA Control: ECLO-2 References: Enterprise System Management STIG Section 3.4.5

Vulnerability Successive logon attempts and/or concurrent sessions per user are not controlled

Vulnerability Discussion Attempted logons must be controlled to hamper password guessing exploits.

Concurrent sessions per individual must be controlled to limit denial of service attacks.

Checks **EGC.0200**

If the ESM permits multiple logon sessions for each user ID. Have ESM administrator show that he has set a maximum.

Default Finding Details The following issues were noted:
Successive logon attempts are not restricted
User is not notified of details of their previous logon
The number of concurrent logon sessions allowed per user is not controlled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0200**

If the ESM permits multiple logon sessions for each user ID. Have ESM administrator define a maximum.

Notes:

EGC.0210 V0008464 CAT III Inadequate Warning Message

8500.2 IA Control: ECWM-1 References: Enterprise System Management STIG Section 3.4.5

Vulnerability Inadequate Warning Message

Vulnerability Discussion A logon banner is used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring, recording and auditing, and that they have no expectation of privacy. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Checks **EGC.0210**

Have the ESM administrator sign onto the application to verify if a warning banner is displayed. If so does it display equivalent to the following information: 1. Use of the application constitutes the user's consent to monitoring. 2. Use of the application is limited to official US Government business only. 3. Unauthorized use is subject to criminal prosecution. 4. Notice that this is a DoD system.

Default Finding Details The following issues were noted:
A warning message does not exist for the application.

The warning message does not include the following:
Use of the application constitutes the users consent to monitoring
Use of the application is limited to official US Government business only
Unauthorized use is subject to criminal prosecution
Notice that this is a DOD system
Users have no expectation of privacy

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0210**

Have the ESM Administrator establish procedures to make sure that all applications that require a user logon, display the proper banner warning screen.

Notes:

EGC.0220 V0008434 CAT II Controlled interface is not used

8500.2 IA Control: ECIC-1

References: Enterprise System Management STIG EGC.0220

Vulnerability Controlled interface is not used

Vulnerability Discussion Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. However, A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks to insure that only predetermined information is passed to the connected system. This safeguard prevents loss or compromise of classified or sensitive information.

Checks **EGC.0220**

Verify with the IAO and ESM administrators that ESM applications are not implemented across DoD information systems operating at different classification levels or across mixed DoD and non DoD systems or networks

Default Finding Details Controlled interface is required but not in use.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0220**

The ESM administrator will validate that the ESM applications being implemented are on DOD systems at the same classification level.

Notes:

EGC.0230 V0008411 CAT II Inadequate Boundary Defense

8500.2 IA Control: EBBD-2

References: Enterprise System Management STIG Section 3.4.5

Vulnerability Inadequate Boundary Defense

Vulnerability Discussion If intrusion detection and intrusion prevention devices are not installed on the host site network, and key boundary points, network and system attacks or compromises cannot be detected or prevented.

Without the Dual-Homed screened subnet (DMZ) architecture traffic that would be normally destined for the DMZ would have to be redirected to the sites internal network. This would allow for a greater opportunity for hackers to exploit.

Checks **EGC.0230**

Verify that all OS-based systems, other than Network IDS', have Host IDS' installed. Note: HIDS are not required on network IDS devices.

Default Finding Details The following issues were noted:
Intrusion detection (NID/JID/RealSecure) devices and intrusion deterrence (Firewall) devices are not installed.
Intrusion detection (NID/JID/RealSecure) devices and intrusion deterrence (Firewall) devices do not cover all key boundary points
A dual-homed screened subnet architecture (DMZ) does not exist or is not being used to protect the enclave as required.
Internet access exists that is not under the control of the enclave manager.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0230**

The IAO will ensure all servers employ host-based IDS, if technically feasible. This requirement may not pertain to legacy systems and cutting edge devices that do not yet have the capability. If a host system cannot technically support a HID, the requirement to employ encryption to the host pursuant to DODI 8500.2 requirements still applies. In these cases, the IAO will mitigate the risk by regular review of audit records for these servers. Documentation must exist from the vendor to approve any variance from this requirement

Notes:

EGC.0240 V0008460 CAT II Integrity mechanisms are not properly employed

8500.2 IA Control: ECTM-2 References: Enterprise System Management STIG Section 3.4.5

Vulnerability Integrity mechanisms are not properly employed

Vulnerability Discussion If integrity checks (hash algorithms and/or checksums) are not used to detect errors in data streams there is no way to ensure the integrity of the application data as it traverses the network.

Checks EGC.0240

Verify with the ESM administrator as to what integrity mechanisms such as parity checks, cyclic redundancy checks, or hash checks are used to ensure the integrity of transmitted data.

Default Finding Details The following issues were noted:
The system does not employ a method to ensure the integrity of input and output files.
Mechanisms are not in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0240

Have the ESM administrator show that documentation exists indicating that a mechanism is used by ESM applications to ensure the integrity of transmitted data.

Notes:

EGC.0250 V0008415 CAT II Insufficiently controlled remote access for privil

8500.2 IA Control: EBRP-1 References: Enterprise System Management STIG Section 3.4.5

Vulnerability Insufficiently controlled remote access for privileged functions. Application is configured to assure session integrity through use of VPN, SSL or another protocol.

Vulnerability Discussion To prevent possible compromise of sensitive information (Privileged logon information) remote access for privileged functions must be discouraged, must be permitted only for compelling operational needs, and must be strictly controlled. In addition to EBRU-1, sessions must employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session must be recorded, and the IAM/O must review the log for every remote session.

Checks **EGC.0250**

Validate with the ESM administrator that the ESM applications are configured with SSL or a follow-on protocol.

EGD.0020

Interview the IAO and ESM SA to determine that a policy is in place to prohibit privileged level access without encryption. ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption (FIPS 140-2 validated}.

EGD.0030

Validate with the ESM administrator that the ESM applications are configured with SSL or a follow-on protocol.

Default Finding Details The following issues were noted:
Remote access for privileged functions is not discouraged.
Remote access for privileged functions is permitted for other than compelling operational needs.
Remote access for privileged functions is not strictly controlled.
Remote access for privileged functions sessions does not employ security measures such as a VPN with blocking mode enabled.
A complete audit trail of each Remote access for privileged functions session is not recorded.
The IAM/O does not review the log of every instance of remote access for privileged functions session on a weekly basis.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGC.0250**

Have the ESM administrator ensure that ESM applications are configured with session protocols that can be implemented using elements of the DoD PKI.

EGD.0020

The IAO will ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption (FIPS 140-2 validated or Type 1), to secure the data traversing the network.

EBRP-1: Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.

EGD.0030

Have the ESM administrator ensure that ESM applications are configured with session protocols that can be implemented using elements of the DoD PKI.

Notes:

EGD.0010 V0004018 CAT II Remote access not IAW DoD Policy.

8500.2 IA Control: EBRP-1, EBRU-1 References: Enterprise System Management STIG Section 3.5

Vulnerability Remote access traffic/data is not secured in accordance with requirements as defined by DoD policy.

Vulnerability Discussion If remote user traffic is allowed to bypass the security architecture to include the IDS, unauthorized access may be undetected and limit the ability of security personnel to stop malicious or unauthorized use of the network. In order to ensure that an attempted or existing attack is noticed, the data from the remote user must be visible to the IDS and firewall.

Checks EGD.0010

Work with the Network reviewer to determine if remote access to the network is in compliance with requirements. Work with all reviewers to determine if remote access to their systems is controlled in accordance with Network requirements.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGD.0010

The NSO will ensure remote access device traffic/data does not bypass the security architecture as outlined in the Network Infrastructure STIG (i.e., all ingress traffic passes through the firewall and NIDS).

EBRU-1: All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.

Notes:

EGD.0040 V0008417 CAT II VPN traffic not visible to IDS

8500.2 IA Control: EBVC-1 References: Enterprise System Management STIG Section 3.5

Vulnerability VPN traffic not visible to IDS

Vulnerability Discussion Intruders can escape detection by hijacking a VPN connection from a trusted enclave or assuming the identity of a trusted user of the VPN

Checks EGD.0040

Interview the network reviewer to validate that the VPN meets compliance with the enclave STIG.

Default Finding Details VPN traffic is not visible to network intrusion detection systems (IDS firewalls).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGD.0040

The NSO will ensure VPNs are established as a full tunnel and VPNs will terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router). Location is not as paramount as being in compliance with DODI 8500.2 EBVC-1 ôVPN traffic is visible to network IDS.ö

Notes:

EGE.0010 V0008475 CAT II Unauthorized physical access

8500.2 IA Control: PECF-2 References: Enterprise System Management STIG Section 3.6

Vulnerability Unauthorized physical access

Vulnerability Discussion To protect classified information, procedures must be developed and enforced to insure that only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.

Checks **EGE.0010**

Work with the Traditional reviewer to determine compliance. Interview the IAO to determine if there is a policy and procedure in place to prohibit unauthorized personnel from gaining access to ESM controlled areas.

Default Finding Details The following issues were noted:
Access list is not maintained
Unauthorized personnel are granted physical access to computing facilities that process classified information
Personnel are granted physical access to computing facilities that process classified information without the appropriate clearance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGE.0010**

The IAO will ensure only authorized personnel with appropriate clearances are granted physical access to ESM computing systems.

Notes:

EGF.0010 V0008367 CAT II Inadequate exercising of COOP/DRP

8500.2 IA Control: COED-2 References: Enterprise System Management STIG Section 3.7

Vulnerability Inadequate exercising of continuity of operations or disaster recovery plans

Vulnerability Discussion If plans are not adequately exercised there can be no assurance they will work when required.

Checks **EGF.0010**

Interview the IAO to determine if a process is in place to exercise COOP and disaster recovery plans in accordance with MAC level requirements.

Default Finding Details The following issues were noted:
last exercise of the COOP or DRP was not within the last 180 days
critical steps of the plan were not exercised.
test of the backup media was not included in the exercise
the exercise plan does not include a strategy for testing all parts of the COOP and DRP over a period of time
simulated events are not incorporated into contingency training to facilitate effective response by personnel in crisis situations
Contingency plan testing is not coordinated with elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
Contingency plans are not tested at the alternate site.
Appropriate officials within the organization did not review the contingency plan test results and initiate corrective actions.

(For Lab tested systems) This requirement is not addressed in the PMs deployment plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGF.0010**

The IAM will ensure that the continuity of operations (COOP) or disaster recovery plans or significant portions are exercised in accordance with the requirements set forth in the DODI 8500.2 for the appropriate MAC level of the systems. COED-2 - COOP, Semi-Annual testing MAC I COED-1 - COOP, Annual testing MAC II and MAC III.

Notes:

EGF.0020 V0008362 CAT II Inadequate Disaster Recovery Plan

8500.2 IA Control: CODP-2

References: Enterprise System Management STIG Section 3.7

Vulnerability Inadequate Disaster Recovery Plan

Vulnerability Discussion Well thought out recovery plans are essential for system recovery and/or business restoration in the event of catastrophic failure or disaster.

Checks **EGF.0020**

Interview the IAO to determine if there is a backup policy in place to ensure backup of critical systems and that backup copies of the Operating Systems other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software. Work with all reviewers to determine compliance with the backup policy. This check does NOT apply to Compliance Validation Visits.

Default Finding Details The following issues were noted:
The Disaster Recovery Plan does not exist
The plan does not provide for partial resumption of mission or business essential function within 24 hours
The plan does not contain business recovery plans
The plan does not contain system contingency plans
The plan does not contain facility disaster recovery plans
The plan has not been officially accepted

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGF.0020**

The IAO will ensure all critical systems, to include infrastructure devices such as routers and inventory records, are backed up and copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software.

Notes:

EGF.0030 V0008360 CAT II Data Backup (redundancy) is inadequate

8500.2 IA Control: CODB-3

References: Enterprise System Management STIG EGF.0030

Vulnerability Data Backup (redundancy) is inadequate

Vulnerability Discussion MAC 1 systems require the capability to continue operation with little or no loss of data or capability should the primary system fail. This feature guarantees the availability of the mission critical IA capability at all times. In order to insure adequate protection against mission failure, the system must mirror the online system as closely as practical, it must be in a separate geographical area, and failover to the redundant system and data must be tested every 6 months.

Checks EGF.0030

Interview the IAO to determine if there is a backup policy in place that ensures data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level. On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data. CODB-3 Data Backup Procedures MAC I Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation. CODB-2 Data Back-up Procedures MAC II Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level. CODB-1 Data Backup Procedures MAC III Data backup is performed at least weekly. This check does NOT apply to Compliance Validation Visits. Work with the reviewers to determine compliance.

Default Finding Details The following issues were noted:
A redundant system is not being used for data backup
The redundant system is not in a separate location
The failover to the redundant system capability is not tested every 6 months

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGF.0030

The IAO will ensure data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level. On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data.

Notes:

EGF.0040 V0008377 CAT II Inadequate Back-up Software

8500.2 IA Control: COSW-1

References: Enterprise System Management STIG Section 3.7

Vulnerability Inadequate Back-up Software

Vulnerability Discussion Inadequate back-up software or improper storage of back-up software can result in extended outages of the information system in the event of a fire or other situation that results in destruction of the operating copy.

Checks EGF.0040

Interview the IAO to determine if there is a backup policy in place to ensure backup of critical systems and that backup copies of the Operating Systems other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software. Work with all reviewers to determine compliance with the backup policy. This check does NOT apply to Compliance Validation Visits.

Default Finding Details The following issues were noted:
There are no back-up copies of the operating system and other critical software
Back-up copies of the operating system and other critical software are collocated with the operational software and not stored in a fire rated container.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGF.0040

The IAO will ensure all critical systems, to include infrastructure devices such as routers and inventory records, are backed up and copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software

Notes:

EGG.0020 V0008510 CAT II Vulnerability Management Program is Inadequate

8500.2 IA Control: VIVM-1

References: Enterprise System Management STIG Section 3.8

Vulnerability Vulnerability Management Program is Inadequate

Vulnerability Discussion Exploiting well-known vulnerabilities is a proven and effective technique followed by malicious users. To combat this, the DOD IAVM program formally announces and tracks the implementation of security specific patches, service releases, hot fixes and system upgrades directed by CINC STRAT through the JTD CNO. Compliance with IAVMs is required unless otherwise directed by system PM. If IAVMs are not complied with, not only is this a violation of DOD policy and procedures, but the site is exposing its most critical systems to attack based upon the exploitation of well-known vulnerabilities. In order to fully comply, each activity must have an active program to identify and fix system vulnerabilities.

Checks **EGG.0020**

A vulnerability management process that includes the timely discovery of patches, testing of patches to ensure interoperability, and installation of the patches is required. Interview the reviewers on the team to determine compliance and the IAO to determine if the process for patch management is being enforced .

Default Finding Details The following issues were noted:
Vulnerability management process does not exist.
Vulnerability management process is ineffective as noted by a high incident of open vulnerabilities.
The vulnerability management process does not include the systematic identification and mitigation of software and hardware vulnerabilities.
Vulnerability mitigation efforts are not independently validated.
Independent validation does not include inspection
Independent validation does not include the use of automated assessment or state management tools
Vulnerability assessment tools have not been acquired
Personnel been not been trained on the assessment tools
Procedures for internal and external assessments have not been developed
Both internal and external assessments are not conducted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EGG.0020**

The IAO will ensure that all security related patches are applied. Some patches may be obtained from the DOD Patch Repository, otherwise contact the vendor. The DOD Patch Repository can be accessed from the following URLs: https://patches.csd.disa.mil for NIPRNet; https://patches.csd.disa.smil.mil for SIPRNet. For additional information on the DOD Patch Repository contact Patch-Support@mont.disa.mil. Additional information and the process for registering devices may be obtained from the the web site located at https://iase.disa.mil.

Notes:

5. CHECKLIST INSTRUCTIONS – SMS Server Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the SMS Server Checks that must be reviewed if reviewing an SMS Server. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

EGA.0040 V0011798 CAT II Unauthorized use of software

8500.2 IA Control: DCPD-1 References: Enterprise System Management STIG Section 3.2.1

Vulnerability Unauthorized use of software. Binary or machine executable public domain software and other software with limited or no warranty (such as those known as freeware or shareware) is not to be used to fulfill an ESM function

Vulnerability Discussion Public domain software is shareware and there cannot be any assurance the products integrity or security mechanisms exist without a code review or vulnerability analysis. Failure to properly authorize shareware before it is installed or used on corporate AISs could result in compromise of sensitive corporate resources.

Checks EGA.0040

The IAO should be interviewed as to the knowledge of any public or freeware software having been installed on the system, and if installed, will provide documented DAA approval.

Default Finding Details The following unauthorized software was identified as being executed on the sytem without DAA approval or with out having been reviewed for requirements relating to IA and IA enabled components.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0040

The IAO will ensure that the acquisition of IA or IA-enabled products meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2.

If not followed IAO will provide a statement indicating
-The software is necessary for mission accomplishment
and there are no alternative IT solutions available.
-The software is assessed for information assurance impacts and approved for use by the DAA.

Notes:

EGA.0110 V0011808 CAT II The ESM version will expire

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability The ESM version will soon expire and become unsupported..

Vulnerability Discussion Vendors do not provide security fixes or software updates to unsupported software versions. Unpatched software allows known vulnerabilities to be exploited.

Checks EGA.0110

Have SA verify with vendor the dates of new releases of the ESM software, the dates support will be dropped on the current running version, and any patches that have not been installed.

Default Finding Details The following ESM products will expire in the next few months:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0110

Have the SA establish procedures to record the version numbers of ESM software every month and log status of current and future versions as to dates when support will be dropped on the current version and verify if any patches have been developed.

Notes:

EGA.0120 V0011807 CAT II An upgrade/migration plan

8500.2 IA Control: DCSW-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability An upgrade/migration plan has not been developed to upgrade an unsupported ESM version to a supported version

Vulnerability Discussion Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack.

Checks EGA.0120

If the check for unsupported version shows an unsupported version or the installed version is within 6 mos. of a drop support notice, then ask if migration plans are in progress to upgrade to a supported version. Make plans to upgrade.

Default Finding Details An upgrade/migration plan has not been developed to address an unsupported ESM software version.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0120

Create an upgrade plan for obsolete or expiring vendor products. As soon as an expiration date is published for the product, prepare to upgrade it. The cost of the upgrade should be budgeted including any additional testing and development required to support the upgrade. A plan for testing the upgrade should also be scheduled. Any other steps for upgrade should be included in the plan and the plan for upgrade should be sceduled for completion prior to expiration of the current product.

Develop an upgrade/migration p (Manual)
Develop an upgrade/migration plan to use a supported version of DBMS software.

Notes:

EGA.0150 V0011812 CAT II (PPS) used by ESM applications is not consistent

8500.2 IA Control: ECSC-1 References: Enterprise System Management STIG Section 3.2.3

Vulnerability (PPS) used by ESM applications is not consistent with secure practices identified in DoD network security guidanceThe site has not blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Vulnerability Discussion Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

Checks EGA.0150

Interview the IAO to determine if there is a procedure in place to identify needed ports and services allowed to traverse the Enclave boundary.
Work with the Network reviewer to determine compliance.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0150

The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Notes:

EGA.0160 V0011813 CAT III Ports and services are not blocked IAW policy.

8500.2 IA Control: COEB-1, COEB-2 References: Enterprise System Management STIG Section 3.2.3

Vulnerability The site has not blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Vulnerability Discussion Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

Checks EGA.0160

Interview the IAO to determine if there is a procedure in place to identify needed ports and services allowed to traverse the Enclave boundary.

Work with the Network reviewer to determine compliance.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0160

The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Notes:

EGB.0040 V0011824 CAT II .Unapproved group authenticators in use

8500.2 IA Control: IAGA-1 References: Enterprise System Management STIG Section 3.3.1

Vulnerability Unapproved group authenticators in use and not approved by the DAA

Vulnerability Discussion Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA). Having group accounts does not allow for proper auditing of who is accessing or changing the network unless an individual authenticator is also used.

Checks EGB.0040

Validate with the IAO that any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA)

Default Finding Details The following issues were noted: Group authenticators are used for access without a tie to an individual authenticator. Group authenticators not based on the DoD PKI has not been explicitly approved by the Designated Approving Authority (DAA).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0040

Validate that any group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA) or removed.

Notes:

EGB.0060 V0011830 CAT III Inadequate encryption of stored sensitive informat

8500.2 IA Control: ECCR-1, ECCR-2, ECCR-3 References: Enterprise System Management STIG Section 3.3.2

Vulnerability Inadequate encryption of stored sensitive information

Vulnerability Discussion If any other user has the ability to write to an I&A database or read authentication credentials, this is a CAT I finding. If non-privileged users can read I&A information other than authentication credentials (e.g., list users but not passwords), this is a CAT III finding.

Checks EGB.0060

The IAO will verify that the vendor of any ESM I & A applications use NIST-certified cryptography to maintain its userid and password database.

Default Finding Details An ESM application that provides internal I&A services, and does not use NIST-certified cryptography to write its I & A database.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0060

Verify If encryption of stored sensitive information is required by the data owner, NIST-certified cryptography must be used.

Notes:

EGC.0110 V0011902 CAT III Inadequate Configuration Management (CM) process

8500.2 IA Control: DCPR-1 References: Enterprise System Management STIG Section 3.4.3

Vulnerability Inadequate Configuration Management (CM) process

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by rigid processes administered by an independent board it much less likely to be in its approved and accredited state.

Checks EGC.0110

Interview the IAO to determine if a Configuration Management (CM) process that follows DODI 8500.2 IA Implementation Policy is used by the ESM application to implement and control changes to the ESM system.

Default Finding Details The following CM issues were noted: There is no formal Configuration Management Process The CM process does not include formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation The CM process does not include a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems The CM process does not include a testing process to verify proposed configuration changes prior to implementation in the operational environment The CM process does not include a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted The organization does not employ automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0110

Verify with the IAO that a Configuration Management (CM) process that follows DODI 8500.2 IA Implementation Policy is created and used by the site if one does not exist. If a (CM) process does exist make sure that ESM utilizes the system for all future changes.

Notes:

EGG.0010 V0011935 CAT II ESM assets and/or systems that support ESM

8500.2 IA Control: VIVM-1 References: Enterprise System Management STIG Section 3.8

Vulnerability ESM assets and/or systems that support ESM protection are not registered with an IAVM tracking mechanism (e.g., Vulnerability Management System (VMS)).

Vulnerability Discussion IAVM tracking mechanisms such as VMS send out notifications on vulnerabilities as they are discovered in commercial and military information infrastructures. If ESM assets are not registered, administrators will not be notified of important vulnerabilities such as viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations. If an assest is not registered, then there is no means by which one can enter, track and resolve vulnerabilities.

Checks EGG.0010

Interview the IAO and review the process to validate whether assets are registered in an IAVM tracking system. The Team Lead will review VMS to see if the system assets have been properly registered. Ask each reviewer if any assets were reviewed that were not in VMS or accurately identified in VMS.

Default Finding Details The following systems are not registered with an IAVM tracking mechanism:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGG.0010

Register all ESM assests in a vulnerability management tracking system.

Notes:

EGG.0020 V0011936 CAT III Security related patches have not been applied to

8500.2 IA Control: VIVM-1 References: Enterprise System Management STIG Section 3.8

Vulnerability Security related patches have not been applied to all ESM systems.

Vulnerability Discussion Patches and fixes to a Computing Applications are necessary elements in maintaining the security posture of a site. If one system has been compromised or exposed to a vulnerability, the entire ESM is at risk.

Checks EGG.0020

A vulnerability management process that includes the timely discovery of patches, testing of patches to ensure interoperability, and installation of the patches is required.

Interview the reviewers on the team to determine compliance and the IAO to determine if the process for patch management is being enforced . For Tivoli verify that they are authorized for install_product or senior in the Tivoli region.

Default Finding Details The following systems are not up to date on critical security patches:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGG.0020

The IAO will ensure that all security related patches are applied. Some patches may be obtained from the DOD Patch Repository, otherwise contact the vendor.

The DOD Patch Repository can be accessed from the following URLs: https://patches.csd.disa.mil for NIPRNet; https://patches.csd.disa.smil.mil for SIPRNet. For additional information on the DOD Patch Repository contact Patch-Support@mont.disa.mil. Additional information and the process for registering devices may be obtained from the the web site located at https://iase.disa.mil.

Notes:

EMS.0010 V0012183 CAT II Access to SMS server software libraries (including

8500.2 IA Control: DCCS-1, DCCS-2, DCSL-1 References: Enterprise System Management STIG Section C.2.1

Vulnerability Access to SMS server software libraries (including executable and configuration files) are not properly restricted.

Vulnerability Discussion The SMS server software libraries include tools that are used for special maintenance tasks. These tools have the capability to significantly impact the operation of an SMS site and clients.

Checks EMS.0010

The SA or IAO will verify that the permissions assigned to the SMS Server software libraries are restricted in accordance with the permissions in the ESM STIG

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below

OBJECT (…\[SMS Folder]),
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS) Permission (Full Control)
(SMS_SiteSystemTo SiteServerConnection_sc) Permission (Read & Execute)
[SMS Limit. Admins] Permission (Full Control)

Default Finding Details The following SMS Server software libraries were not properly protected:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0010

The SA or the IAO will modify the settings to be compliant with the ESM STIG.

Notes:

EMS.0030 V0012192 CAT II Access to SMS are not properly restricted

8500.2 IA Control: DCCS-1, DCCS-2, DCSL-1 References: Enterprise System Management STIG Section C.2.1

Vulnerability Access to SMS ACL Reset, Hierarchy Maintenance, and Remote Tools program are not properly restricted.

Vulnerability Discussion SMS software libraries include tools that are used for special maintenance tasks. These tools have the capability to significantly impact the operation of an SMS site and clients and could be used to corrupt the ESM systems and clients.

Checks EMS.0030

The SA or IAO will verify that the permissions assigned to the SMS Tool libraries are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified Below:
OBJECT (…\[SMS Folder]\bin\…\ACLreset.exe),
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
Object (…\[SMS Folder]\bin\…\PreInst.exe)
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
OBJECT (…\[SMS Folder]\bin\…\Remote.exe)
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)

Default Finding Details The following SMS tools libraries were not properly protected:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0030

The SA or the IAO will modify the permissions to be compliant with the ESM STIG.

Notes:

EMS.0040 V0012196 CAT II SMS Site Server, Site Database Server

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability SMS Site Server, Site Database Server, and an other Site System is installed on a windows domain controller.

Vulnerability Discussion SMS server service (SMS Executive) must be a member of the Administrators group for the machine on which it runs. If the SMS server software was installed on a Windows domain controller machine, it would gain domain-wide Administrator privileges.

Checks EMS.0040

Have the SA verify that the SMS Site Servers are not installed on a Windows domain controller machines.

Default Finding Details The SMS Server service was installed on a windows domain controller

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0040

Make sure that when planning the installation of SMS, that the SMS Executive software is not sharing a server that is running a Windows Domain Controller.

Notes:

EMS.0050 V0012197 CAT II The instance of SQL Server on SMS Site Database

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability The instance of SQL Server on the SMS Site Database Server is not dedicated to SMS.

Vulnerability Discussion The SMS Site Database Server should be installed on the same machine as the Site Server. Combining these roles reduces exposure of SMS data on the network, reduces authentication transactions, and simplifies security administration.

Checks **EMS.0050**

Verify with the SA that the SMS Site database Server is installed on the same system as MS SQL Server.

Default Finding Details The SMS Site Database server was not installed on the same machine as the Site SQL Server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0050**

The SMS System adminastrator will plan to configure the system to contain the SMS Site Server with the MS SQL Server.

Notes:

EMS.0060 V0012198 CAT III Roles requiring IIS wer enabled on the Site Server

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability Roles requiring IIS were enabled on the SMS Site Server machine.

Vulnerability Discussion The site server's computer account has administrative privileges on other computers. IIS runs by using the LocalSystem account, which is the only account with the right to use the computer account. This typically is the case only on site servers. When using advanced security, the SMS site server manages its local files and registry entries by using the LocalSystem account. Software running in the LocalSystem account context of IIS has equal access to those files and registry entries.

Checks **ESM.0060**

Verify with the SMS System adminastrator that IIS and the Site Server roles are kept separated.

Default Finding Details Roles requiring IIS were enabled on the SMS Site Server Machine.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0060**

The ESM adminastrator will make sure that he/she does not put the Site Server on a Computer with IIS.

Notes:

EMS.0070 V0012215 CAT II The SMS Management Point is enabled

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability The SMS Management Point is enabled on the Site Server machine running as a single site environments with Advanced Clients and without the Active Directory extensions.

Vulnerability Discussion SMS uses a variety of site systems with specialized functions. Advanced Clients interact with management points. Management points interact with the site server and the SMS site database server. Clients might need a server locator point to find a management point. This unavoidably increases the attack surface of SMS across the enterprise. Failure to secure site servers, management points, CAPs, and SMS site database servers could allow an attacker to spoof site systems and distribute unauthorized software to SMS clients. Improperly secured site systems could also lead to a compromise of the site server.

Checks **EMS.0070**

Verify with the ESM administrator that SMS Management point is not enabled on the Site Server machine in a single site environment with Advanced Clients, without Active Directory extensions.

Default Finding Details The SMS Management point was enabled on the Site server machine.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0070**

The ESM administrator will remove the management point off the site server machine if this environment exists.

Notes:

EMS.0080 V0012216 CAT II Unaproved usage of PPSM-designated ports

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability Unaproved usage of PPSM-designated RED or YELLOW ports

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **ESM.0080**

Verify with the IAO that the DAA has approved usage of any and all ports used by SMS.

Default Finding Details The following ports were not approved.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **ESM.0080**

The IAO will make sure that a process is in place to follow the DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM).

Notes:

EMS.0090 V0012221 CAT II Reporting Point server not configured to use

8500.2 IA Control: ECNK-1, ECNK-2 References: Enterprise System Management STIG Section C.2.2

Vulnerability Reporting Point server not configured to use the HyperText Transfer Protocol Secure (HTTPS) protocol or an alternate network encryption mechanism. .

Vulnerability Discussion Passwords and Userids transmitted in clear text are easily hijacked and can be used to violate the integrity of the systems.

Checks **EMS.0090**

Verify with the ESM administrator that the Reporting Point server is using encryption to transmit data.

Default Finding Details The reporting point server failed to use encryption to transmit data.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0090**

The ESM administrator will install a DOD approved encryption on the Reporting Point server.

Notes:

EMS.0100 V0012225 CAT III SMS Executive service name not changed

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section C.2.2

Vulnerability SMS Executive service name not changed from SMSService

Vulnerability Discussion Due to the power of the SMS systems it is recommended that Default names should be changed and password ptotected to avoid entry and control of SMS controlled systems.

Checks **EMS.0100**

Attempt to logon to SMS Executive service using SMSService.

Default Finding Details SMS Executive Service name not changed from SMSService

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0100**

ESM administrator will validate that all factory set passwords are removed from the system.

Notes:

EMS.0110 V0012226 CAT II Access to SMS server data directories and files

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to SMS server data directories and files are not properly restricted.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks EMS.0110

Verify that SMS server data directories and files is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:
OBJECT (…\[SMS Data Folder])
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission(Full Control)
(SMS_SiteSystemTo SQLConnection_ sc) Permission(Full Control)
[SQL Server account] Permission(Full Control)

Default Finding Details The following data sets or files have invalid permissions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0110

The SA will update the permissions for SMS server data directories and files with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0120 V0012227 CAT III Access to SMS server data directories and files

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to SMS client data directories and files are not properly restricted.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks **EMS.0120**

Verify that SMS client data directories and files is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:
OBJECT (…\[SMS Data Folder])
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission(Full Control)
(SMS_SiteSystemTo SQLConnection_ sc) Permission(Full Control)
[SQL Server account] Permission(Full Control)

Default Finding Details The following data sets or files have invalid permissions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0120**

The SA will update the permissions for SMS server data directories and files with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0130 V0012229 CAT III Access to shared SMS folders on SMS servers

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to shared SMS folders on SMS servers is not properly restricted

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks EMS.0130

Verify that SMS folders on SMS servers are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.
1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:

OBJECT (…\[SMS Folder])
Account Assignment (Administrators) Permission (Full Control)

OBJECT (SMS_[sc])
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

OBJECT (SMS_Site)
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

OBJECT (SMSClient)
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

Default Finding Details The following SMS folders on SMS servers were not properly restricted:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0130

The SA will update the permissions for SMS folders on SMS servers with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0140 V0012231 CAT II WMI namespaces on SMS servers and clients

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability WMI namespaces on SMS servers and clients are not properly protected.

Vulnerability Discussion WMI incorporates methods and data structures related to system management. Therefore access to WMI methods and data is a security concern for SMS. WMI data is stored in logical structures known as namespaces. Unauthorized access to these structures could expose the integrity of the system.

Checks EMS.0140

Have the SA verify that WMI namespaces on SMS servers and clients is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.
1. Use the WMI MS Management Cconsole (MMC) via 'start| run | wmimgmt.msc' to get to the properties page.

2. Then click the Security tab.

3. Verify that the permissions match those specified below:

NAMESPACE (Root)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\CCM)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\CIMV2)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\SMS)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)
(SMS Admins) Permission (Execute Methods, Provider Write, Enable Account, Remote Enable)
([SMS Limit. Admins]) Permission (Execute Methods, Provider Write, Enable Account, Remote Enable)

NAMESPACE (NetworkModel)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

Default Finding Details Access to the following WMI namespaces were not properly restricted:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0140

The SA will update the permissions for SMS WMI namespaces on SMS servers and clients in accordance with the permissions in Appendix C.3.

Notes:

EMS.0150 V0012232 CAT II The SMS Legacy Client has been installed

8500.2 IA Control: DCCS-2, IAIA-1, IAIA-2, DCCS-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability The SMS Legacy Client has been installed on an SMS system.

Vulnerability Discussion Legacy Clients use privileged Windows user accounts for key tasks such as installing software on clients. Managing Windows application accounts is an administrative burden and potential source of vulnerability. If an application account is assigned a weak password and the account is compromised, the confidentiality, integrity, and availability of the application could be negatively impacted. When the account is privileged, entire platforms can be affected. For an ESM application such as SMS, this could be the enabling factor in a major security incident. In addition to the Windows account management issues and the Microsoft support statement, Legacy Clients do not include the support found in the Advanced Client to authenticate SMS data using digital signatures.

Checks EMS.0150

Interview the SMS administrator to verify that the SMS legacy client is not installed on the system.

From Admin console:
In the SMS Administrator console, you can determine the client version and type by viewing the properties of computers in collections and queries. The ClientType property is 0 if the client is a Legacy Client and 1 if the client is an Advanced Client. These are properties of the SMS_R_System class and the v_SMS_R_System view. You can use this information when creating queries and reports.

From Client conole:
You can determine the client version by opening Control Panel, opening Systems Management, and then clicking the Components tab.

If you need to determine the client version by using a script or any other programmatic method, you can locate the client version in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Client Components\ SMS Client Base Components\Installation Properties|Installed Version

On the Advanced Client, this client's version registry key value is set to 99.9.9999.9999. This value ensures that the Advanced Client software is never overwritten by the Legacy Client software. To determine the client's software version, you can check Windows Management Instrumentation (WMI). The client's software version is stored in the ClientVersion property of the SMS_Client class in the root\CCM namespace.

At a client, you can determine the client type by the SMS client installation directory. If a %Windir%\MS\SMS directory exists, then the client is a Legacy Client. If a %Windir%\System32\CCM\Clicomp directory exists, then the client is an Advanced Client. Also, Systems Management in Control Panel on the Advanced Client has an Actions tab, which the Legacy Client does not have.

Default Finding Details SMS Legacy Client has been installed on the following systems:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0150

The SMS administrator will use advanced client when installing SMS on a systems.

Notes:

EMS.0160 V0012240 CAT II SMS accounts were defined in a Windows admin

8500.2 IA Control: DCCS-1, DCCS-2, ECAN-1, ECCD-1, ECCD-2

References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS accounts were defined in a Windows administrator-level group on a domain controller.

Vulnerability Discussion Most SMS accounts can be defined on local systems where they are used. This helps reduce the attack surface that is presented by these accounts. The notable exception to this strategy is the SMS Service account. This account is used in several contexts (such as SMS Discovery) that require Windows domain access. Defining these accounts in an administrator group on a domain controller will increase exposure if it is hijacked.

Checks **EMS.0160**

Verify with the SA that no SMS accounts are defined in any Windows administrator-level group on a domain controller, for any of the following accounts SMS Service, Server Connection, Site Address, Site System Database, Site System Connection, and Remote Service.

Default Finding Details The following SMS accounts were found defined in a Windows administrator-level group on a domain controller

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0160**

The SA will see that SMS accounts defined in any Windows administrator-level group on a domain controller are removed

Notes:

EMS.0170 V0012241 CAT II SMS Service account

8500.2 IA Control: DCCS-1, DCCS-2, ECAN-1, ECCD-1, ECCD-2

References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS Service account is used for the supported functions of Site System Connection and Site Address accounts, Site Address and Site System Connection accounts should be defined.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Buy assingning accounts to a lower privelege level reduces the risk associated with hijacked accounts.

Checks **EMS.0170**

The SMS Administrator will verify that separation of duties was enforced by assingning seperate accounts for Site System Connection and Site Address.

Default Finding Details The SMS Sevice account was used to support Site System Connection and Site Address account functions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0170**

The SA will make sure that separation of duties and least privilege principles are enforced on the SMS systems.

Notes:

EMS.0180 V0012255 CAT II The SMS Advanced Client Network Access account

8500.2 IA Control: DCCS-1, DCCS-2, ECLP-1 References: Enterprise System Management STIG Setion C.2.3.2

Vulnerability The SMS Advanced Client Network Access account is defined in a Windows administrator-level group on a domain controller.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system

Checks **EMS.0180**

The SA will ensure that separation of duties and least privilege principles are used when defining the SMS Advanced Client Network Access account..

Default Finding Details The following SMS Advanced Client Network Access account is defined in a Windows administrator-level group on a domain controller.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0180**

The SA will verify that Separation of duties and least privilege principles are enforced on the SMS systems.

Notes:

EMS.0190 V0012263 CAT II Failure to assign a Client Push Install account

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Failure to assign a Client Push Installation account

Vulnerability Discussion The Client Push Installation account may have Windows administrator-level privileges over a wide span of clients. To mitigate the risk associated with this definition, organizations should consider disabling this account for periods when it is not being used. If client push is used and this account is not defined it will default to the SMS Service account and could not be diabled when not in use.

Checks **EMS.0190**

The SMS administrator will verify that if the client push function is used, and that it has been assigned its own account. The SMS Administrator will verify tht this account is disabled when not in being used.

Default Finding Details The clent push installation account was not defined for SMS.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0190**

The SA will validate that Separation of duties and least privilege principles are being used for SMS accounts.

Notes:

EMS.0200 V0012272 CAT II Internal Microsoft SQL Server accounts

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Internal Microsoft SQL Server accounts (such as the SA pseudo database account) is being used as an SMS Site Database account.

Vulnerability Discussion Seperation of the SMS Site Database account reduces the exposure by allowing the SMS accout to do just functions assocciated with the SMS database.

Checks EMS.0200

Have the SMS Administrator verify that the SMS Site Database account has been assigned a seperate account from the SQL database account.

Default Finding Details The SMS Site Database account was not defined seperately from the Microsoft SQL Server account.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0200

Have the SA verify that a Separation of duties and least privilege principles are practiced on the SMS system and that account codes are created to seperate and reduce the privileges for all accounts.

Notes:

EMS.0210 V0012283 CAT III SMS Legacy Client accounts are not defined

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS Legacy Client accounts are defined or are not properly disabled.

Vulnerability Discussion It is important that any client legacy accounts that are specified in the EMS STIG are deleted or disabled to avoid using them to violate the integrity on any of the systems that they are defined on.

Checks EMS.0210

The SA will validate that the following SMS legacy client accounts have been deleted or disabled Client Connection, Client Services (DC), Client Services (non-DC), Client User Token (DC), Client User Token (non-DC), CCM Boot Loader (DC), CCM Boot Loader (non DC).
NOTE: The letters DC represent domain controller.

Default Finding Details The following accounts that were to be deleted or disabled were found on SMS Clients:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0210

The SA will see that all SMS legacy client accounts are either disabled or deleted.

Notes:

EMS.0220 V0012287 CAT II SMS administrator accounts are not documented

8500.2 IA Control: PRNK-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS administrator accounts are not documented

Vulnerability Discussion SMS Administrators have power over the SMS Applications. ESM applications commonly perform sensitive functions, requiring elevated privileges, on multiple hosts. Some of these functions, such as security patch management, are essential to operations because they help to maintain secure environments. The conclusion from these facts is that security controls on ESM applications are critical. Administrtors of these products need to be tightly controlled.

Checks **EMS.0220**

The IAO will validate that all SMS administrators are authorized and have a valid DD2875 on file.

Default Finding Details The following SMS administrators were not documented with the IAO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0220**

The IAO will validate that all SMS administrators accounts are authorized and have valid DD2875 forms filed.

Notes:

EMS.0230 V0012301 CAT II Accounts other than SMS application accounts

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Accounts other than SMS application accounts or SMS server computer accounts are members of the Site System to Site Server Connection, Site System to SQL Server Connection, and Site-to-Site Connection Windows groups.

Vulnerability Discussion Access to SMS privileges and data can be assigned to groups that represent roles associated with SMS operations. Using these groups in a role based access control strategy can be more efficient and secure than assigning access rights to individual accounts.

Checks **EMS.0230**

The SA will validate that only SMS application accounts or SMS server computer accounts are inluded into the Site System to Site Server Connection, Site System to SQL Server Connection, and Site-to-Site Connection Windows groups. To allow enforcement by discretionary or role-based access.

Default Finding Details The following accounts were inappropriately assigned to the Site System to Site Server Connection, Site System to SQL Server Connection, or Site-to-Site Connection Windows groups.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0230**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0240 V0012303 CAT II Accounts other than documented SMS reporting user

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Accounts other than documented SMS reporting users are members of the Reporting Users group.

Vulnerability Discussion Access to SMS privileges and data can be assigned to groups that represent roles associated with SMS operations. Using these groups in a role based access control strategy can be more efficient and secure than assigning access rights to individual accounts.

Checks **EMS.0240**

The SA will validate that only SMS reporting users are members of the Reporting Users group.

Default Finding Details The following accounts were inappropriately included as members of the Reporting Users group:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0240**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0250 V0012325 CAT III The Legacy Clients Internal Client Group Windows

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability The Legacy Clients Internal Client Group Windows group is defined.

Vulnerability Discussion The Legacy Client in Microsoft ®Systems Management Server (SMS) is not considered a secure environment. Any groups that are not used should therefore be removed.

Checks **EMS.0250**

The SA will validate that all legacy groups that are not being used are deleted.

Default Finding Details The Legacy Clients Internal Client Group Windows group is defined.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0250**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0260 V0012330 CAT III Component Status and Site System Status

8500.2 IA Control: ECAR-1, ECAR-2, ECAR-3 References: Enterprise System Management STIG Section C.2.3.4

Vulnerability The Component Status and Site System Status summarizers are disabled and no alternate on-line monitoring capability is installed

Vulnerability Discussion Minimum Audit record content is required to insure detection, attribution and recovery from changes to DOD Information and systems.

Checks EMS.0260

The SMS administrator will validate that the Component Status and Site System Status summarizers are enabled or an alternate on-line monitoring capability is maintained.

Default Finding Details The SMS system does perform proper security audit and logging functions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0260

The IAO will insure that all systems perform recording of audit information. Audit messages will provide an audit trail of actions taken in the SMS Administrator console that result in objects being added, modified, or deleted.

Notes:

EMS.0270 V0012337 CAT II The Component Status and Site System Status

8500.2 IA Control: ECAT-1, ECAT-2 References: Enterprise System Management STIG Section C.2.3.4

Vulnerability The Component Status and Site System Status summarizers data or their alternates data are not regularly reviewed for indications of inappropriate or unusual activity.

Vulnerability Discussion Audit records for all sources are regularly reviewed and suspected violations of IA Policies must be analyzed and reported. For critical and classified systems, an automated, continuous on-line monitoring and audit trail creation capability must be deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks EMS.0270

The SMS administrator or IAO will validate that audit information is regularly reviewed.

Default Finding Details The Component Status and Site System Status summarizers audit records or their alternates are not regularly reviewed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0270

The IAO will verify that procedures exist for timely reviews of SMS audit record.

Notes:

EMS.0280 V0012385 CAT II Audit records not properly retained

8500.2 IA Control: ECRR-1

References: Enterprise System Management STIG Section C.2.3.4

Vulnerability Audit records not properly retained

Vulnerability Discussion Audit records are used to track any compromise of SMS data. Failure to backup and save this data would impact the investigation of such compromises.

Checks **EMS.0280**

The SA will provide verification that SMS audit data is backed up and archived daily. Prior to the data being lost or overwritten.

Default Finding Details The SMS audit data was not backed up prior to being lost or overwritten.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0280**

The SA will validate that procedures exist on the SMS system for backup and archiving of SMS audit data.

Notes:

EMS.0290 V0012413 CAT III Inadequate Warning Message

8500.2 IA Control: ECWM-1

References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Inadequate Warning Message

Vulnerability Discussion A logon banner is used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring, recording and auditing, and that they have no expectation of privacy. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Checks **EMS.0290**

The SMS administrator will logon to access the Report Viewer web application on the SMS Reporting Point site system to validate to the reviewer that a valid logon banner page is presented.

Default Finding Details The following issues were noted: A warning message does not exist for the application. The warning message does not include the following: Use of the application constitutes the users consent to monitoring Use of the application is limited to official US Government business only Unauthorized use is subject to criminal prosecution Notice that this is a DOD system Users have no expectation of privacy

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0290**

The SA will validate that a logon banner page exists for all DOD systems that are accessed from remote sites.

Notes:

EMS.0300 V0012416 CAT II Acceptence of unsigned data from sites running SMS

8500.2 IA Control: ECCT-2, ECCT-1 References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Acceptence of unsigned data from sites running SMS 2.0 SP4 and earlier was permitted

Vulnerability Discussion The loss of integrity for SMS data transmitted between servers and clients can result in a number of problems. Data corruption in the SMS Site Database could result in invalid information being used to administer clients. It could be possible for clients to receive malicious code or data that would cause a loss of their confidentiality, integrity, or availability characteristics.

Checks EMS.0300

Have the SMS Administrator verify that unsigned communication is disabled from sites that are running SMS 2.0 SP4 and earlier.

Disabling Unsigned Communications Between Sites.

1. In the SMS Administrator console, navigate to the site's node.

Systems Management Server

Site Database (site code - site name)

Site Hierarchy

(site code - site name)

2. Right-click the site, and then select Properties.

3. In the Site Properties dialog box, click the Advanced tab, and then select Do not accept unsigned data from sites that are running SMS 2.0 SP4 and earlier.

Default Finding Details Unsigned communications between sites option was not disabled for sites running SMS 2.0 SP4 and earlier

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0300

The SA will validate that the system will not accept unsigned data from sites that are running SMS 2.0 SP4 and earlier.

Notes:

EMS.0310 V0012429 CAT II Require secure key exchange between sites

8500.2 IA Control: ECCT-1, ECCT-2 References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Require secure key exchange between sites. Site Properties option is disabled

Vulnerability Discussion The loss of integrity for SMS data transmitted between servers and clients can result in a number of problems. Data corruption in the SMS Site Database could result in invalid information being used to administer clients. It could be possible for clients to receive malicious code or data that would cause a loss of their confidentiality, integrity, or availability characteristics.

Checks EMS.0310

The SMS administrator will verify that the secure key exchange between sites" Site Properties option is enabled.

To require secure key exchange between sites

1. In the SMS Administrator console, navigate to the site's node.

Systems Management Server

Site Database (site code - site name)

Site Hierarchy

(site code - site name)

2. Right-click the site, and then click Properties.

3. In the Site Properties dialog box, click the Advanced tab, and then select Require secure key exchange between sites.

Default Finding Details Secure key exchange between sites" Site Properties option is disabled

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0310

The SA will ensure that the secure key exchange between sites is enabled for all SMS systems running at SMS 2.0 SP5.

Notes:

EMS.0320 V0012458 CAT II The Backup SMS Site Server task was not enabled.

8500.2 IA Control: CODP-1, CODP-2, CODP-3 References: Enterprise System Management STIG Section C.2.6

Vulnerability The Backup SMS Site Server task was not enabled.

Vulnerability Discussion When an SMS site fails, it is important that you are able to quickly recover that site with as little data loss as possible. Backing up sites in your hierarchy is the most important step to ensure a minimum data loss, and a successful recovery in case of a site failure. Although it is possible to recover sites without a backup snapshot, recovering a site with a backup snapshot ensures the least data loss and a less complex recovery process.
To ensure that backing up a site is as easy as possible, SMS provides the Backup SMS Site Server task, referred to as the SMS backup task. This is a predefined maintenance task, and you can enable and configure the SMS backup task from the SMS Administrator console.

Checks **EMS.0320**

The SMS Administrator will verify that the Backup SMS Site Server task is enabled and properly configured.

Default Finding Details The Backup SMS Site Server task was not enabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0320**

The SA will ensure that a Continuity plan is set up for the SMS To ensure that the availability of SMS is maintained and in accordance with the DODI 8500.2 IA controls for Disaster and Recovery Planning.

Notes:

EMS.0330 V0012459 CAT II Logging is not enabled for the SMS_SITE_BACKUP

8500.2 IA Control: ECAR-1, ECAR-2, ECAR-3 References: Enterprise System Management STIG Section C.2.6

Vulnerability Logging is not enabled for the SMS_SITE_BACKUP service.

Vulnerability Discussion Minimum Audit record content is required to insure detection, attribution and recovery from changes to DOD Information and systems.

Checks **EMS.0330**

The EMS administrator will verify that logging is enabled for SMS_SITE_BACKUP service.

Default Finding Details Logging is not enabled for the SMS_SITE_BACKUP service.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0330**

The SA will validate that logging is enabled for the SMS_SITE_BACKUP service.

Notes:

EMS.0340 V0012460 CAT II The parent SMS backup directory

8500.2 IA Control: CODP-2 References: Enterprise System Management STIG Section C.2.6

Vulnerability The parent SMS backup directory is located on the same logical drive partition as the parent SMS data directory.

Vulnerability Discussion Failure to use a separate volume or location to backup the SMS backup from the Parent system would make the backup vulnerable to any hardware problems encountered on that volume.

Checks EMS.0340

The SMS administrator will verify that backup copies of SMS System data sets are allocated to a separate logical volume.

Default Finding Details The SMS System was not backed up on a seperate volume from the parent system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0340

The SA will validate that all system backups are performed to separate volumes from the data being saved.

Notes:

EMS.0350 V0012461 CAT II SMS backup directories and files are restricted

8500.2 IA Control: ECCD-2, COBR-1, ECCD-1 References: Enterprise System Management STIG Section C.2.6

Vulnerability SMS backup directories and files are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

Vulnerability Discussion System Backups should be limited to only authorized users, to protect the integrity and confidentiality of the data.

Checks EMS.0350

The SA will ensure that system backups are restricted to authorized personnel, with the permissions indicated in Appendix C.3. of the ESM STIG.
1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:

OBJECT ([SITE_BACKUP_DESTINATION]),
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission (Full Control)

Default Finding Details The following unautorized logons had access to the SMS backup data.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0350

The SA will validate that the SMS backup data is Protected in accordance with the DODI 8500.2 IA control for Backup Copies of Critical Software.

Notes:

6. CHECKLIST INSTRUCTIONS – SMS Client Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the SMS Client Checks that must be reviewed if reviewing an SMS Client. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

EGA.0040 V0011798 CAT II Unauthorized use of software

8500.2 IA Control: DCPD-1 References: Enterprise System Management STIG Section 3.2.1

Vulnerability Unauthorized use of software. Binary or machine executable public domain software and other software with limited or no warranty (such as those known as freeware or shareware) is not to be used to fulfill an ESM function

Vulnerability Discussion Public domain software is shareware and there cannot be any assurance the products integrity or security mechanisms exist without a code review or vulnerability analysis. Failure to properly authorize shareware before it is installed or used on corporate AISs could result in compromise of sensitive corporate resources.

Checks EGA.0040

The IAO should be interviewed as to the knowledge of any public or freeware software having been installed on the system, and if installed, will provide documented DAA approval.

Default Finding Details The following unauthorized software was identified as being executed on the sytem without DAA approval or with out having been reviewed for requirements relating to IA and IA enabled components.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0040

The IAO will ensure that the acquisition of IA or IA-enabled products meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2.

If not followed IAO will provide a statement indicating
-The software is necessary for mission accomplishment
and there are no alternative IT solutions available.
-The software is assessed for information assurance impacts and approved for use by the DAA.

Notes:

EGA.0110 V0011808 CAT II The ESM version will expire

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability The ESM version will soon expire and become unsupported..

Vulnerability Discussion Vendors do not provide security fixes or software updates to unsupported software versions. Unpatched software allows known vulnerabilities to be exploited.

Checks EGA.0110

Have SA verify with vendor the dates of new releases of the ESM software, the dates support will be dropped on the current running version, and any patches that have not been installed.

Default Finding Details The following ESM products will expire in the next few months:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0110

Have the SA establish procedures to record the version numbers of ESM software every month and log status of current and future versions as to dates when support will be dropped on the current version and verify if any patches have been developed.

Notes:

EGA.0120 V0011807 CAT II An upgrade/migration plan

8500.2 IA Control: DCSW-1 References: Enterprise System Management STIG Section 3.2.2

Vulnerability An upgrade/migration plan has not been developed to upgrade an unsupported ESM version to a supported version

Vulnerability Discussion Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack.

Checks EGA.0120

If the check for unsupported version shows an unsupported version or the installed version is within 6 mos. of a drop support notice, then ask if migration plans are in progress to upgrade to a supported version. Make plans to upgrade.

Default Finding Details An upgrade/migration plan has not been developed to address an unsupported ESM software version.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0120

Create an upgrade plan for obsolete or expiring vendor products. As soon as an expiration date is published for the product, prepare to upgrade it. The cost of the upgrade should be budgeted including any additional testing and development required to support the upgrade. A plan for testing the upgrade should also be scheduled. Any other steps for upgrade should be included in the plan and the plan for upgrade should be sceduled for completion prior to expiration of the current product.

Develop an upgrade/migration p (Manual)
Develop an upgrade/migration plan to use a supported version of DBMS software.

Notes:

EGA.0150 V0011812 CAT II (PPS) used by ESM applications is not consistent

8500.2 IA Control: ECSC-1 References: Enterprise System Management STIG Section 3.2.3

Vulnerability (PPS) used by ESM applications is not consistent with secure practices identified in DoD network security guidanceThe site has not blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Vulnerability Discussion Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

Checks EGA.0150

Interview the IAO to determine if there is a procedure in place to identify needed ports and services allowed to traverse the Enclave boundary.
Work with the Network reviewer to determine compliance.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0150

The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Notes:

EGA.0160 V0011813 CAT III Ports and services are not blocked IAW policy.

8500.2 IA Control: COEB-1, COEB-2 References: Enterprise System Management STIG Section 3.2.3

Vulnerability The site has not blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Vulnerability Discussion Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

Checks EGA.0160

Interview the IAO to determine if there is a procedure in place to identify needed ports and services allowed to traverse the Enclave boundary.

Work with the Network reviewer to determine compliance.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGA.0160

The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.

Reference the Network Infrastructure STIG to obtain additional configuration guidance for required PPS blocking at the Enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

Notes:

EGB.0040 V0011824 CAT II .Unapproved group authenticators in use

8500.2 IA Control: IAGA-1 References: Enterprise System Management STIG Section 3.3.1

Vulnerability Unapproved group authenticators in use and not approved by the DAA

Vulnerability Discussion Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA). Having group accounts does not allow for proper auditing of who is accessing or changing the network unless an individual authenticator is also used.

Checks EGB.0040

Validate with the IAO that any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA)

Default Finding Details The following issues were noted: Group authenticators are used for access without a tie to an individual authenticator. Group authenticators not based on the DoD PKI has not been explicitly approved by the Designated Approving Authority (DAA).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0040

Validate that any group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA) or removed.

Notes:

EGB.0060 V0011830 CAT III Inadequate encryption of stored sensitive informat

8500.2 IA Control: ECCR-1, ECCR-2, ECCR-3 References: Enterprise System Management STIG Section 3.3.2

Vulnerability Inadequate encryption of stored sensitive information

Vulnerability Discussion If any other user has the ability to write to an I&A database or read authentication credentials, this is a CAT I finding. If non-privileged users can read I&A information other than authentication credentials (e.g., list users but not passwords), this is a CAT III finding.

Checks EGB.0060

The IAO will verify that the vendor of any ESM I & A applications use NIST-certified cryptography to maintain its userid and password database.

Default Finding Details An ESM application that provides internal I&A services, and does not use NIST-certified cryptography to write its I & A database.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGB.0060

Verify If encryption of stored sensitive information is required by the data owner, NIST-certified cryptography must be used.

Notes:

EGC.0110 V0011902 CAT III Inadequate Configuration Management (CM) process

8500.2 IA Control: DCPR-1 References: Enterprise System Management STIG Section 3.4.3

Vulnerability Inadequate Configuration Management (CM) process

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by rigid processes administered by an independent board it much less likely to be in its approved and accredited state.

Checks EGC.0110

Interview the IAO to determine if a Configuration Management (CM) process that follows DODI 8500.2 IA Implementation Policy is used by the ESM application to implement and control changes to the ESM system.

Default Finding Details The following CM issues were noted: There is no formal Configuration Management Process The CM process does not include formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation The CM process does not include a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems The CM process does not include a testing process to verify proposed configuration changes prior to implementation in the operational environment The CM process does not include a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted The organization does not employ automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGC.0110

Verify with the IAO that a Configuration Management (CM) process that follows DODI 8500.2 IA Implementation Policy is created and used by the site if one does not exist. If a (CM) process does exist make sure that ESM utilizes the system for all future changes.

Notes:

EGG.0010 V0011935 CAT II ESM assets and/or systems that support ESM

8500.2 IA Control: VIVM-1 References: Enterprise System Management STIG Section 3.8

Vulnerability ESM assets and/or systems that support ESM protection are not registered with an IAVM tracking mechanism (e.g., Vulnerability Management System (VMS)).

Vulnerability Discussion IAVM tracking mechanisms such as VMS send out notifications on vulnerabilities as they are discovered in commercial and military information infrastructures. If ESM assets are not registered, administrators will not be notified of important vulnerabilities such as viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations. If an assest is not registered, then there is no means by which one can enter, track and resolve vulnerabilities.

Checks EGG.0010

Interview the IAO and review the process to validate whether assets are registered in an IAVM tracking system. The Team Lead will review VMS to see if the system assets have been properly registered. Ask each reviewer if any assets were reviewed that were not in VMS or accurately identified in VMS.

Default Finding Details The following systems are not registered with an IAVM tracking mechanism:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGG.0010

Register all ESM assests in a vulnerability management tracking system.

Notes:

EGG.0020 V0011936 CAT III Security related patches have not been applied to

8500.2 IA Control: VIVM-1 References: Enterprise System Management STIG Section 3.8

Vulnerability Security related patches have not been applied to all ESM systems.

Vulnerability Discussion Patches and fixes to a Computing Applications are necessary elements in maintaining the security posture of a site. If one system has been compromised or exposed to a vulnerability, the entire ESM is at risk.

Checks EGG.0020

A vulnerability management process that includes the timely discovery of patches, testing of patches to ensure interoperability, and installation of the patches is required.

Interview the reviewers on the team to determine compliance and the IAO to determine if the process for patch management is being enforced . For Tivoli verify that they are authorized for install_product or senior in the Tivoli region.

Default Finding Details The following systems are not up to date on critical security patches:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGG.0020

The IAO will ensure that all security related patches are applied. Some patches may be obtained from the DOD Patch Repository, otherwise contact the vendor.

The DOD Patch Repository can be accessed from the following URLs: https://patches.csd.disa.mil for NIPRNet; https://patches.csd.disa.smil.mil for SIPRNet. For additional information on the DOD Patch Repository contact Patch-Support@mont.disa.mil. Additional information and the process for registering devices may be obtained from the the web site located at https://iase.disa.mil.

Notes:

EMS.0030 V0012192 CAT II Access to SMS are not properly restricted

8500.2 IA Control: DCCS-1, DCCS-2, DCSL-1 References: Enterprise System Management STIG Section C.2.1

Vulnerability Access to SMS ACL Reset, Hierarchy Maintenance, and Remote Tools program are not properly restricted.

Vulnerability Discussion SMS software libraries include tools that are used for special maintenance tasks. These tools have the capability to significantly impact the operation of an SMS site and clients and could be used to corrupt the ESM systems and clients.

Checks EMS.0030

The SA or IAO will verify that the permissions assigned to the SMS Tool libraries are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified Below:
OBJECT (…\[SMS Folder]\bin\…\ACLreset.exe),
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
Object (…\[SMS Folder]\bin\…\PreInst.exe)
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
OBJECT (…\[SMS Folder]\bin\…\Remote.exe)
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)

Default Finding Details The following SMS tools libraries were not properly protected:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0030

The SA or the IAO will modify the permissions to be compliant with the ESM STIG.

Notes:

EMS.0050 V0012197 CAT II The instance of SQL Server on SMS Site Database

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability The instance of SQL Server on the SMS Site Database Server is not dedicated to SMS.

Vulnerability Discussion The SMS Site Database Server should be installed on the same machine as the Site Server. Combining these roles reduces exposure of SMS data on the network, reduces authentication transactions, and simplifies security administration.

Checks EMS.0050

Verify with the SA that the SMS Site database Server is installed on the same system as MS SQL Server.

Default Finding Details The SMS Site Database server was not installed on the same machine as the Site SQL Server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0050

The SMS System adminastrator will plan to configure the system to contain the SMS Site Server with the MS SQL Server.

Notes:

EMS.0060 V0012198 CAT III Roles requiring IIS wer enabled on the Site Server

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability Roles requiring IIS were enabled on the SMS Site Server machine.

Vulnerability Discussion The site server's computer account has administrative privileges on other computers. IIS runs by using the LocalSystem account, which is the only account with the right to use the computer account. This typically is the case only on site servers. When using advanced security, the SMS site server manages its local files and registry entries by using the LocalSystem account. Software running in the LocalSystem account context of IIS has equal access to those files and registry entries.

Checks **ESM.0060**

Verify with the SMS System adminastrator that IIS and the Site Server roles are kept separated.

Default Finding Details Roles requiring IIS were enabled on the SMS Site Server Machine.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0060**

The ESM adminastrator will make sure that he/she does not put the Site Server on a Computer with IIS.

Notes:

EMS.0070 V0012215 CAT II The SMS Management Point is enabled

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability The SMS Management Point is enabled on the Site Server machine running as a single site environments with Advanced Clients and without the Active Directory extensions.

Vulnerability Discussion SMS uses a variety of site systems with specialized functions. Advanced Clients interact with management points. Management points interact with the site server and the SMS site database server. Clients might need a server locator point to find a management point. This unavoidably increases the attack surface of SMS across the enterprise. Failure to secure site servers, management points, CAPs, and SMS site database servers could allow an attacker to spoof site systems and distribute unauthorized software to SMS clients. Improperly secured site systems could also lead to a compromise of the site server.

Checks **EMS.0070**

Verify with the ESM administrator that SMS Management point is not enabled on the Site Server machine in a single site environment with Advanced Clients, without Active Directory extensions.

Default Finding Details The SMS Management point was enabled on the Site server machine.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0070**

The ESM administrator will remove the management point off the site server machine if this environment exists.

Notes:

EMS.0080 V0012216 CAT II Unaproved usage of PPSM-designated ports

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section C.2.1

Vulnerability Unaproved usage of PPSM-designated RED or YELLOW ports

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **ESM.0080**

Verify with the IAO that the DAA has approved usage of any and all ports used by SMS.

Default Finding Details The following ports were not approved.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **ESM.0080**

The IAO will make sure that a process is in place to follow the DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM).

Notes:

EMS.0090 V0012221 CAT II Reporting Point server not configured to use

8500.2 IA Control: ECNK-1, ECNK-2 References: Enterprise System Management STIG Section C.2.2

Vulnerability Reporting Point server not configured to use the HyperText Transfer Protocol Secure (HTTPS) protocol or an alternate network encryption mechanism. .

Vulnerability Discussion Passwords and Userids transmitted in clear text are easily hijacked and can be used to violate the integrity of the systems.

Checks **EMS.0090**

Verify with the ESM administrator that the Reporting Point server is using encryption to transmit data.

Default Finding Details The reporting point server failed to use encryption to transmit data.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0090**

The ESM administrator will install a DOD approved encryption on the Reporting Point server.

Notes:

EMS.0100 V0012225 CAT III SMS Executive service name not changed

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section C.2.2

Vulnerability SMS Executive service name not changed from SMSService

Vulnerability Discussion Due to the power of the SMS systems it is recommended that Default names should be changed and password ptotected to avoid entry and control of SMS controlled systems.

Checks EMS.0100

Attempt to logon to SMS Executive service using SMSService.

Default Finding Details SMS Executive Service name not changed from SMSService

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0100

ESM administrator will validate that all factory set passwords are removed from the system.

Notes:

EMS.0110 V0012226 CAT II Access to SMS server data directories and files

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to SMS server data directories and files are not properly restricted.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks EMS.0110

Verify that SMS server data directories and files is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:
OBJECT (…\[SMS Data Folder])
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission(Full Control)
(SMS_SiteSystemTo SQLConnection_ sc) Permission(Full Control)
[SQL Server account] Permission(Full Control)

Default Finding Details The following data sets or files have invalid permissions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0110

The SA will update the permissions for SMS server data directories and files with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0120 V0012227 CAT III Access to SMS server data directories and files

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to SMS client data directories and files are not properly restricted.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks **EMS.0120**

Verify that SMS client data directories and files is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:
OBJECT (…\[SMS Data Folder])
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission(Full Control)
(SMS_SiteSystemTo SQLConnection_ sc) Permission(Full Control)
[SQL Server account] Permission(Full Control)

Default Finding Details The following data sets or files have invalid permissions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0120**

The SA will update the permissions for SMS server data directories and files with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0130 V0012229 CAT III Access to shared SMS folders on SMS servers

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability Access to shared SMS folders on SMS servers is not properly restricted

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time. - Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability. - Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

Checks EMS.0130

Verify that SMS folders on SMS servers are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.
1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:

OBJECT (…\[SMS Folder])
Account Assignment (Administrators) Permission (Full Control)

OBJECT (SMS_[sc])
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

OBJECT (SMS_Site)
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

OBJECT (SMSClient)
Account Assignment (Authenticated Users) Permission (Change)
(Domain Computers) Permission (Change)

Default Finding Details The following SMS folders on SMS servers were not properly restricted:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0130

The SA will update the permissions for SMS folders on SMS servers with the permissions documented in Appendix C.3. of the ESM STIG.

Notes:

EMS.0140 V0012231 CAT II WMI namespaces on SMS servers and clients

8500.2 IA Control: DCCS-1, DCCS-2, ECCD-1, ECCD-2 References: Enterprise System Management STIG Section C.2.3.1

Vulnerability WMI namespaces on SMS servers and clients are not properly protected.

Vulnerability Discussion WMI incorporates methods and data structures related to system management. Therefore access to WMI methods and data is a security concern for SMS. WMI data is stored in logical structures known as namespaces. Unauthorized access to these structures could expose the integrity of the system.

Checks EMS.0140

Have the SA verify that WMI namespaces on SMS servers and clients is restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.
1. Use the WMI MS Management Cconsole (MMC) via 'start| run | wmimgmt.msc' to get to the properties page.

2. Then click the Security tab.

3. Verify that the permissions match those specified below:

NAMESPACE (Root)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\CCM)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\CIMV2)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

NAMESPACE (Root\SMS)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)
(SMS Admins) Permission (Execute Methods, Provider Write, Enable Account, Remote Enable)
([SMS Limit. Admins]) Permission (Execute Methods, Provider Write, Enable Account, Remote Enable)

NAMESPACE (NetworkModel)
Account Assignment (Administrators) Permission (all)
(Authenticated Users) Permission (Execute Methods, Provider Write, Enable Account)

Default Finding Details Access to the following WMI namespaces were not properly restricted:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0140

The SA will update the permissions for SMS WMI namespaces on SMS servers and clients in accordance with the permissions in Appendix C.3.

Notes:

EMS.0150 V0012232 CAT II The SMS Legacy Client has been installed

8500.2 IA Control: DCCS-2, IAIA-1, IAIA-2, DCCS-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability The SMS Legacy Client has been installed on an SMS system.

Vulnerability Discussion Legacy Clients use privileged Windows user accounts for key tasks such as installing software on clients. Managing Windows application accounts is an administrative burden and potential source of vulnerability. If an application account is assigned a weak password and the account is compromised, the confidentiality, integrity, and availability of the application could be negatively impacted. When the account is privileged, entire platforms can be affected. For an ESM application such as SMS, this could be the enabling factor in a major security incident. In addition to the Windows account management issues and the Microsoft support statement, Legacy Clients do not include the support found in the Advanced Client to authenticate SMS data using digital signatures.

Checks EMS.0150

Interview the SMS administrator to verify that the SMS legacy client is not installed on the system.

From Admin console:
In the SMS Administrator console, you can determine the client version and type by viewing the properties of computers in collections and queries. The ClientType property is 0 if the client is a Legacy Client and 1 if the client is an Advanced Client. These are properties of the SMS_R_System class and the v_SMS_R_System view. You can use this information when creating queries and reports.

From Client conole:
You can determine the client version by opening Control Panel, opening Systems Management, and then clicking the Components tab.

If you need to determine the client version by using a script or any other programmatic method, you can locate the client version in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Client Components\ SMS Client Base Components\Installation Properties|Installed Version

On the Advanced Client, this client's version registry key value is set to 99.9.9999.9999. This value ensures that the Advanced Client software is never overwritten by the Legacy Client software. To determine the client's software version, you can check Windows Management Instrumentation (WMI). The client's software version is stored in the ClientVersion property of the SMS_Client class in the root\CCM namespace.

At a client, you can determine the client type by the SMS client installation directory. If a %Windir%\MS\SMS directory exists, then the client is a Legacy Client. If a %Windir%\System32\CCM\Clicomp directory exists, then the client is an Advanced Client. Also, Systems Management in Control Panel on the Advanced Client has an Actions tab, which the Legacy Client does not have.

Default Finding Details SMS Legacy Client has been installed on the following systems:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0150

The SMS administrator will use advanced client when installing SMS on a systems.

Notes:

EMS.0160 V0012240 CAT II SMS accounts were defined in a Windows admin

8500.2 IA Control: DCCS-1, DCCS-2, ECAN-1, ECCD-1, ECCD-2

References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS accounts were defined in a Windows administrator-level group on a domain controller.

Vulnerability Discussion Most SMS accounts can be defined on local systems where they are used. This helps reduce the attack surface that is presented by these accounts. The notable exception to this strategy is the SMS Service account. This account is used in several contexts (such as SMS Discovery) that require Windows domain access. Defining these accounts in an administrator group on a domain controller will increase exposure if it is hijacked.

Checks EMS.0160

Verify with the SA that no SMS accounts are defined in any Windows administrator-level group on a domain controller, for any of the following accounts SMS Service, Server Connection, Site Address, Site System Database, Site System Connection, and Remote Service.

Default Finding Details The following SMS accounts were found defined in a Windows administrator-level group on a domain controller

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0160

The SA will see that SMS accounts defined in any Windows administrator-level group on a domain controller are removed

Notes:

EMS.0170 V0012241 CAT II SMS Service account

8500.2 IA Control: DCCS-1, DCCS-2, ECAN-1, ECCD-1, ECCD-2

References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS Service account is used for the supported functions of Site System Connection and Site Address accounts, Site Address and Site System Connection accounts should be defined.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Buy assingning accounts to a lower privelege level reduces the risk associated with hijacked accounts.

Checks EMS.0170

The SMS Administrator will verify that separation of duties was enforced by assingning seperate accounts for Site System Connection and Site Address.

Default Finding Details The SMS Sevice account was used to support Site System Connection and Site Address account functions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0170

The SA will make sure that separation of duties and least privilege principles are enforced on the SMS systems.

Notes:

EMS.0180 V0012255 CAT II The SMS Advanced Client Network Access account

8500.2 IA Control: DCCS-1, DCCS-2, ECLP-1 References: Enterprise System Management STIG Setion C.2.3.2

Vulnerability The SMS Advanced Client Network Access account is defined in a Windows administrator-level group on a domain controller.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system

Checks EMS.0180

The SA will ensure that separation of duties and least privilege principles are used when defining the SMS Advanced Client Network Access account..

Default Finding Details The following SMS Advanced Client Network Access account is defined in a Windows administrator-level group on a domain controller.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0180

The SA will verify that Separation of duties and least privilege principles are enforced on the SMS systems.

Notes:

EMS.0190 V0012263 CAT II Failure to assign a Client Push Install account

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Failure to assign a Client Push Installation account

Vulnerability Discussion The Client Push Installation account may have Windows administrator-level privileges over a wide span of clients. To mitigate the risk associated with this definition, organizations should consider disabling this account for periods when it is not being used. If client push is used and this account is not defined it will default to the SMS Service account and could not be diabled when not in use.

Checks EMS.0190

The SMS administrator will verify that if the client push function is used, and that it has been assigned its own account. The SMS Administrator will verify tht this account is disabled when not in being used.

Default Finding Details The clent push installation account was not defined for SMS.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0190

The SA will validate that Separation of duties and least privilege principles are being used for SMS accounts.

Notes:

EMS.0200 V0012272 CAT II Internal Microsoft SQL Server accounts

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Internal Microsoft SQL Server accounts (such as the SA pseudo database account) is being used as an SMS Site Database account.

Vulnerability Discussion Seperation of the SMS Site Database account reduces the exposure by allowing the SMS accout to do just functions assocciated with the SMS database.

Checks EMS.0200

Have the SMS Administrator verify that the SMS Site Database account has been assigned a seperate account from the SQL database account.

Default Finding Details The SMS Site Database account was not defined seperately from the Microsoft SQL Server account.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0200

Have the SA verify that a Separation of duties and least privilege principles are practiced on the SMS system and that account codes are created to seperate and reduce the privileges for all accounts.

Notes:

EMS.0210 V0012283 CAT III SMS Legacy Client accounts are not defined

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS Legacy Client accounts are defined or are not properly disabled.

Vulnerability Discussion It is important that any client legacy accounts that are specified in the EMS STIG are deleted or disabled to avoid using them to violate the integrity on any of the systems that they are defined on.

Checks EMS.0210

The SA will validate that the following SMS legacy client accounts have been deleted or disabled Client Connection, Client Services (DC), Client Services (non-DC), Client User Token (DC), Client User Token (non-DC), CCM Boot Loader (DC), CCM Boot Loader (non DC).
NOTE: The letters DC represent domain controller.

Default Finding Details The following accounts that were to be deleted or disabled were found on SMS Clients:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0210

The SA will see that all SMS legacy client accounts are either disabled or deleted.

Notes:

EMS.0220 V0012287 CAT II SMS administrator accounts are not documented

8500.2 IA Control: PRNK-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability SMS administrator accounts are not documented

Vulnerability Discussion SMS Administrators have power over the SMS Applications. ESM applications commonly perform sensitive functions, requiring elevated privileges, on multiple hosts. Some of these functions, such as security patch management, are essential to operations because they help to maintain secure environments. The conclusion from these facts is that security controls on ESM applications are critical. Administrtors of these products need to be tightly controlled.

Checks **EMS.0220**

The IAO will validate that all SMS administrators are authorized and have a valid DD2875 on file.

Default Finding Details The following SMS administrators were not documented with the IAO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0220**

The IAO will validate that all SMS administrators accounts are authorized and have valid DD2875 forms filed.

Notes:

EMS.0230 V0012301 CAT II Accounts other than SMS application accounts

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Accounts other than SMS application accounts or SMS server computer accounts are members of the Site System to Site Server Connection, Site System to SQL Server Connection, and Site-to-Site Connection Windows groups.

Vulnerability Discussion Access to SMS privileges and data can be assigned to groups that represent roles associated with SMS operations. Using these groups in a role based access control strategy can be more efficient and secure than assigning access rights to individual accounts.

Checks **EMS.0230**

The SA will validate that only SMS application accounts or SMS server computer accounts are inluded into the Site System to Site Server Connection, Site System to SQL Server Connection, and Site-to-Site Connection Windows groups. To allow enforcement by discretionary or role-based access.

Default Finding Details The following accounts were inappropriately assigned to the Site System to Site Server Connection, Site System to SQL Server Connection, or Site-to-Site Connection Windows groups.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0230**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0240 V0012303 CAT II Accounts other than documented SMS reporting user

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability Accounts other than documented SMS reporting users are members of the Reporting Users group.

Vulnerability Discussion Access to SMS privileges and data can be assigned to groups that represent roles associated with SMS operations. Using these groups in a role based access control strategy can be more efficient and secure than assigning access rights to individual accounts.

Checks **EMS.0240**

The SA will validate that only SMS reporting users are members of the Reporting Users group.

Default Finding Details The following accounts were inappropriately included as members of the Reporting Users group:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0240**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0250 V0012325 CAT III The Legacy Clients Internal Client Group Windows

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section C.2.3.2

Vulnerability The Legacy Clients Internal Client Group Windows group is defined.

Vulnerability Discussion The Legacy Client in Microsoft ®Systems Management Server (SMS) is not considered a secure environment. Any groups that are not used should therefore be removed.

Checks **EMS.0250**

The SA will validate that all legacy groups that are not being used are deleted.

Default Finding Details The Legacy Clients Internal Client Group Windows group is defined.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0250**

The IAO will ensure that Access to classified or sensitive data is not granted without verifying need-to-know and Access is enforced by discretionary or role-based access controls.

Notes:

EMS.0260 V0012330 CAT III Component Status and Site System Status

8500.2 IA Control: ECAR-1, ECAR-2, ECAR-3 References: Enterprise System Management STIG Section C.2.3.4

Vulnerability The Component Status and Site System Status summarizers are disabled and no alternate on-line monitoring capability is installed

Vulnerability Discussion Minimum Audit record content is required to insure detection, attribution and recovery from changes to DOD Information and systems.

Checks EMS.0260

The SMS administrator will validate that the Component Status and Site System Status summarizers are enabled or an alternate on-line monitoring capability is maintained.

Default Finding Details The SMS system does perform proper security audit and logging functions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0260

The IAO will insure that all systems perform recording of audit information. Audit messages will provide an audit trail of actions taken in the SMS Administrator console that result in objects being added, modified, or deleted.

Notes:

EMS.0270 V0012337 CAT II The Component Status and Site System Status

8500.2 IA Control: ECAT-1, ECAT-2 References: Enterprise System Management STIG Section C.2.3.4

Vulnerability The Component Status and Site System Status summarizers data or their alternates data are not regularly reviewed for indications of inappropriate or unusual activity.

Vulnerability Discussion Audit records for all sources are regularly reviewed and suspected violations of IA Policies must be analyzed and reported. For critical and classified systems, an automated, continuous on-line monitoring and audit trail creation capability must be deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected. This is to protect Critical DOD Systems from possible harm and/or exploitation and to protect Critical DOD Information.

Checks EMS.0270

The SMS administrator or IAO will validate that audit information is regularly reviewed.

Default Finding Details The Component Status and Site System Status summarizers audit records or their alternates are not regularly reviewed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0270

The IAO will verify that procedures exist for timely reviews of SMS audit record.

Notes:

EMS.0280 V0012385 CAT II Audit records not properly retained

8500.2 IA Control: ECRR-1

References: Enterprise System Management STIG Section C.2.3.4

Vulnerability Audit records not properly retained

Vulnerability Discussion Audit records are used to track any compromise of SMS data. Failure to backup and save this data would impact the investigation of such compromises.

Checks **EMS.0280**

The SA will provide verification that SMS audit data is backed up and archived daily. Prior to the data being lost or overwritten.

Default Finding Details The SMS audit data was not backed up prior to being lost or overwritten.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0280**

The SA will validate that procedures exist on the SMS system for backup and archiving of SMS audit data.

Notes:

EMS.0290 V0012413 CAT III Inadequate Warning Message

8500.2 IA Control: ECWM-1

References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Inadequate Warning Message

Vulnerability Discussion A logon banner is used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring, recording and auditing, and that they have no expectation of privacy. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Checks **EMS.0290**

The SMS administrator will logon to access the Report Viewer web application on the SMS Reporting Point site system to validate to the reviewer that a valid logon banner page is presented.

Default Finding Details The following issues were noted: A warning message does not exist for the application. The warning message does not include the following: Use of the application constitutes the users consent to monitoring Use of the application is limited to official US Government business only Unauthorized use is subject to criminal prosecution Notice that this is a DOD system Users have no expectation of privacy

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0290**

The SA will validate that a logon banner page exists for all DOD systems that are accessed from remote sites.

Notes:

EMS.0300 V0012416 CAT II Acceptence of unsigned data from sites running SMS

8500.2 IA Control: ECCT-2, ECCT-1 References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Acceptence of unsigned data from sites running SMS 2.0 SP4 and earlier was permitted

Vulnerability Discussion The loss of integrity for SMS data transmitted between servers and clients can result in a number of problems. Data corruption in the SMS Site Database could result in invalid information being used to administer clients. It could be possible for clients to receive malicious code or data that would cause a loss of their confidentiality, integrity, or availability characteristics.

Checks EMS.0300

Have the SMS Administrator verify that unsigned communication is disabled from sites that are running SMS 2.0 SP4 and earlier.

Disabling Unsigned Communications Between Sites.

1. In the SMS Administrator console, navigate to the site's node.

Systems Management Server

Site Database (site code - site name)

Site Hierarchy

(site code - site name)

2. Right-click the site, and then select Properties.

3. In the Site Properties dialog box, click the Advanced tab, and then select Do not accept unsigned data from sites that are running SMS 2.0 SP4 and earlier.

Default Finding Details Unsigned communications between sites option was not disabled for sites running SMS 2.0 SP4 and earlier

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0300

The SA will validate that the system will not accept unsigned data from sites that are running SMS 2.0 SP4 and earlier.

Notes:

EMS.0310 V0012429 CAT II Require secure key exchange between sites

8500.2 IA Control: ECCT-1, ECCT-2 References: Enterprise System Management STIG Section C.2.3.5

Vulnerability Require secure key exchange between sites. Site Properties option is disabled

Vulnerability Discussion The loss of integrity for SMS data transmitted between servers and clients can result in a number of problems. Data corruption in the SMS Site Database could result in invalid information being used to administer clients. It could be possible for clients to receive malicious code or data that would cause a loss of their confidentiality, integrity, or availability characteristics.

Checks EMS.0310

The SMS administrator will verify that the secure key exchange between sites" Site Properties option is enabled.

To require secure key exchange between sites

1. In the SMS Administrator console, navigate to the site's node.

Systems Management Server

Site Database (site code - site name)

Site Hierarchy

(site code - site name)

2. Right-click the site, and then click Properties.

3. In the Site Properties dialog box, click the Advanced tab, and then select Require secure key exchange between sites.

Default Finding Details Secure key exchange between sites" Site Properties option is disabled

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0310

The SA will ensure that the secure key exchange between sites is enabled for all SMS systems running at SMS 2.0 SP5.

Notes:

EMS.0320 V0012458 CAT II The Backup SMS Site Server task was not enabled.

8500.2 IA Control: CODP-1, CODP-2, CODP-3 References: Enterprise System Management STIG Section C.2.6

Vulnerability The Backup SMS Site Server task was not enabled.

Vulnerability Discussion When an SMS site fails, it is important that you are able to quickly recover that site with as little data loss as possible. Backing up sites in your hierarchy is the most important step to ensure a minimum data loss, and a successful recovery in case of a site failure. Although it is possible to recover sites without a backup snapshot, recovering a site with a backup snapshot ensures the least data loss and a less complex recovery process.
To ensure that backing up a site is as easy as possible, SMS provides the Backup SMS Site Server task, referred to as the SMS backup task. This is a predefined maintenance task, and you can enable and configure the SMS backup task from the SMS Administrator console.

Checks **EMS.0320**

The SMS Administrator will verify that the Backup SMS Site Server task is enabled and properly configured.

Default Finding Details The Backup SMS Site Server task was not enabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0320**

The SA will ensure that a Continuity plan is set up for the SMS To ensure that the availability of SMS is maintained and in accordance with the DODI 8500.2 IA controls for Disaster and Recovery Planning.

Notes:

EMS.0330 V0012459 CAT II Logging is not enabled for the SMS_SITE_BACKUP

8500.2 IA Control: ECAR-1, ECAR-2, ECAR-3 References: Enterprise System Management STIG Section C.2.6

Vulnerability Logging is not enabled for the SMS_SITE_BACKUP service.

Vulnerability Discussion Minimum Audit record content is required to insure detection, attribution and recovery from changes to DOD Information and systems.

Checks **EMS.0330**

The EMS administrator will verify that logging is enabled for SMS_SITE_BACKUP service.

Default Finding Details Logging is not enabled for the SMS_SITE_BACKUP service.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **EMS.0330**

The SA will validate that logging is enabled for the SMS_SITE_BACKUP service.

Notes:

EMS.0340 V0012460 CAT II The parent SMS backup directory

8500.2 IA Control: CODP-2 References: Enterprise System Management STIG Section C.2.6

Vulnerability The parent SMS backup directory is located on the same logical drive partition as the parent SMS data directory.

Vulnerability Discussion Failure to use a separate volume or location to backup the SMS backup from the Parent system would make the backup vulnerable to any hardware problems encountered on that volume.

Checks EMS.0340

The SMS administrator will verify that backup copies of SMS System data sets are allocated to a separate logical volume.

Default Finding Details The SMS System was not backed up on a seperate volume from the parent system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0340

The SA will validate that all system backups are performed to separate volumes from the data being saved.

Notes:

EMS.0350 V0012461 CAT II SMS backup directories and files are restricted

8500.2 IA Control: ECCD-2, COBR-1, ECCD-1 References: Enterprise System Management STIG Section C.2.6

Vulnerability SMS backup directories and files are restricted in accordance with the permissions in Appendix C.3. of the ESM STIG.

Vulnerability Discussion System Backups should be limited to only authorized users, to protect the integrity and confidentiality of the data.

Checks EMS.0350

The SA will ensure that system backups are restricted to authorized personnel, with the permissions indicated in Appendix C.3. of the ESM STIG.
1. Open Windows Explorer, and then locate the file or folder for which you want to check permissions

2. Right-click the file or folder, click Properties, and then click the Security tab.

3. Verify that the permissions match those specified below:

OBJECT ([SITE_BACKUP_DESTINATION]),
Account Assignment (Administrator) Permission (Full Control)
(System) Permission(Full Control)
(SMS Admins) Permission (Full Control)

Default Finding Details The following unautorized logons had access to the SMS backup data.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EMS.0350

The SA will validate that the SMS backup data is Protected in accordance with the DODI 8500.2 IA control for Backup Copies of Critical Software.

Notes:

7. CHECKLIST INSTRUCTIONS – Tivoli Management Enterprise Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Management Enterprise Checks that must be reviewed if reviewing Tivoli Management Enterprise. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks **TME.0001**

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TME.0001**

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

8. CHECKLIST INSTRUCTIONS – Tivoli Management Framework Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Management Framework Checks that must be reviewed if reviewing Tivoli Management Framework. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

EGG.0020 V0011936 CAT III Security related patches have not been applied to

8500.2 IA Control: VIVM-1 References: Enterprise System Management STIG Section 3.8

Vulnerability Security related patches have not been applied to all ESM systems.

Vulnerability Discussion Patches and fixes to a Computing Applications are necessary elements in maintaining the security posture of a site. If one system has been compromised or exposed to a vulnerability, the entire ESM is at risk.

Checks EGG.0020

A vulnerability management process that includes the timely discovery of patches, testing of patches to ensure interoperability, and installation of the patches is required.

Interview the reviewers on the team to determine compliance and the IAO to determine if the process for patch management is being enforced . For Tivoli verify that they are authorized for install_product or senior in the Tivoli region.

Default Finding Details The following systems are not up to date on critical security patches:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes EGG.0020

The IAO will ensure that all security related patches are applied. Some patches may be obtained from the DOD Patch Repository, otherwise contact the vendor.

The DOD Patch Repository can be accessed from the following URLs: https://patches.csd.disa.mil for NIPRNet; https://patches.csd.disa.smil.mil for SIPRNet. For additional information on the DOD Patch Repository contact Patch-Support@mont.disa.mil. Additional information and the process for registering devices may be obtained from the the web site located at https://iase.disa.mil.

Notes:

TEC.0011 V0012905 CAT II TEC.0011

8500.2 IA Control: COTR-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate Recovery Procedures

Vulnerability Discussion Improper system recovery can result in loss or compromise of sensitive information and/or compromise of the system by unauthorized individuals who seize the opportunity to exploit known vulnerabilities. Tivoli requires a trusted recovery of the TMR, policy regions, managed nodes and gateways in the event of a technical failure.

Checks TEC.0011

The TMR administrator, TEC administrator and Tivoli administrators will maintain documentation as part of the disaster recovery plan describing the procedures necessary to perform a trusted recovery of the TEC to include the event server, database, adapter files, software and configuration files.

Default Finding Details The following issues were noted: Recovery procedures and technical system features do not exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are not documented. Circumstances that can inhibit trusted recover are documented but appropriate mitigating procedures are not in place. There is no list of personnel authorized to perform the recover function.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0012

Insure that the DRP or SOP has recovery procedures that indicate the steps needed for secure recovery. Verification process can include original COTS or GOTS installation media or a hash of the installation program. These procedures should include any special considerations for trusted recovery such as network attachment or placement. The procedure should also include the list of authorized personnel that perform the function.

Notes:

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks **TME.0001**

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TME.0001**

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0003 V0012779 CAT II TMF.0003

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.2.1

Vulnerability TMF software not being protected from unauthorized use.

Vulnerability Discussion The TMF software is very powerful and must be protected from unathorized use, to avoid attacks on other systems or introduction of unathorized code.

Checks **TMF.0003**

Have the IAO verify that all software modules and libraries are restricted to ESM authorized users

Default Finding Details The following software libraries were not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0003**

Have the IAO validate that all libraries containing TMF modules are properly protected and open only to authorized users.

Notes:

TMF.0006 V0012901 CAT II TMF.0006

8500.2 IA Control: DCSD-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate IA Documentation

Vulnerability Discussion If the DAA, IAM/IAO are not performing assigned functions in accordance with DoD requirements, it could impact the overall security of the facility, personnel, systems, and data, which could lead to degraded security. If the DAA, IAM/IAO are not appointed in writing, there will be no way to ensure they understand the responsibilities of the position and the appointment criteria. The lack of a complete System Security Plan could lead to ineffective secure operations and impede accreditation.

Checks TMF.0006

Interview the IAM to ensure a System Security Plan is established and describes the technical, administrative, and procedural IA program and policies that govern the Tivoli Management Environment (TME)/TMR. Verify that procedures exist for such activities as the distribution of software patches and new releases, hardware, software and network monitoring, backup and recovery, and user administration.

Default Finding Details The following issues were noted: Required IA roles are not established in writing. (DAA, IAM/IAO) Appointments of required IA Roles do not include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan does not exist; It should be Appendix s of the SSAA System Security Plan does not include the following required information: Description of the technical, administrative, and procedural IA program and policies that govern the DoD information system Identification of all IA personnel Specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0006

Prior to installing and setting up an ESM environment verify that a System Security Plan has been established, that cover the items mentioned above.

Notes:

TMF.0007 V0012900 CAT II TMF.0007

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.1

Vulnerability Systems hosting TIVOLI Sostware will be configured as specified in the ESM STIG.

Vulnerability Discussion Due to the capabilities of TIVOLI software to alter information on the systems it controls. It is important to properly secure the TIVOLI software.

Checks TMF.0007

Verify with the IAM that the Tivoli software was installed following the configuration specified in the ESM STIG and the STIG of the system it was installed on. If installed on WINDOWS or UNIX systems, verify that physical security of the platforms, network connectivity, file access controls, change management and backups and recovery be addressed so as to ensure the confidentiality, availability and integrity of the Tivoli Enterprise and the resources that exist in it.

Default Finding Details The following TIVOLI Managegment software was not configued as specified in the ESM STIG and the STIG of the system it was installed on.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0007

When installing TIVOLI software validate that it is configred as specified in the ESM STIG and the STIG of the system it was installed on.

Notes:

TMF.0009 V0012902 CAT III TMF.0009

8500.2 IA Control: DCCT-1 References: Enterprise System Management STIG Section B.2.1

Vulnerability Inadequate Deployment Procedures

Vulnerability Discussion Undocumented procedures for upgrading or deploying new hardware, software or software upgrades for Tivoli systems can lead to inconsistent deployments which can cause incompatibility problems between devices and systems and/or possible security holes. These problems or holes can lead to slowdowns or outages on the network or unauthorized access or attacks on DoD assets.

Checks **TMF.0009**

The IAO will Ensure procedures exist which address the testing and implementation process for all patches, upgrades and AIS deployments.
The procedures should be in the Configuration Management Plan.
For Lab tested systems ensure the PM details the testing and release process and addresses change control in the PM's deployment plan.

Default Finding Details Procedures which address the testing and implementation process for all patches, upgrades and AIS deployments do not exist

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0009**

The IAO will ensure that procedures are documented in the configuration Management Plan.

Notes:

TMF.0010 V0012903 CAT III TMF.0010

8500.2 IA Control: CODP-2 References: Enterprise System Management STIG Section b.2.1

Vulnerability Inadequate Disaster Recovery Plan

Vulnerability Discussion Disaster Recovery Plan does not allow for the resumption of mission or business critical functions within 24 hours.

Checks **TMF.0010**

The IAM will ensure that a written plan exists that addresses the partial resumption of mission or business essential functions with 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Default Finding Details Well thought out recovery plans are essential for system recovery and/or business restoral in the event of catastrophic failure or disaster.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0010**

The Tivoli administrator must Develop a Disaster Recovery Plan for the Information System or Facility that Insures the plan:
provides for partial resumption of function within 24 hours
contains business recovery plans
contains system contingency plans
contains facility disaster recovery plans
is officially accepted by the IS or facility owner

Notes:

TMF.0011 V0012904 CAT III TMF.0011

8500.2 IA Control: COED-1

References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate exercising of continuity of operations or disaster recovery plans

Vulnerability Discussion Failure to test disaster recovery plans. If plans are not adequately exercised there can be no assurance they will work when required.

Checks TMF.0011

Obtain the last DRP report from the IAM. Examine the report of the COOP or DRP to ensure it was performed within the last 365 days and that critical steps of the plan were exercised. Ensure a test of the backup media was included in the exercise. Ensure the exercise plan includes a strategy for testing all parts of the COOP and DRP over a period of time. Verify that appropriate officials within the organization review the contingency plan test results and initiate corrective actions. (NIST CP-4) Verify that the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan). (NIST CP-4)

Default Finding Details The following issues were noted: Last exercise of the COOP or DRP was not within the last 365 days Critical steps of the plan were not exercised. Test of the backup media was not included in the exercise The exercise plan does not include a strategy for testing all parts of the COOP and DRP over a period of time No evidence found that appropriate officials within the organization did not review the contingency plan test results and initiate corrective actions. No evidence found that the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0011

Set up procedures to insure the COOP or DRP is exercised annually and that critical steps of the plan are exercised. Ensure a test of the backup media is included in the exercise. Ensure the exercise plan includes a strategy for testing all parts of the COOP and DRP over a period of time.
Ensure that appropriate officials within the organization review the contingency plan test results and initiate corrective actions. Ensure that the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan.

Notes:

TMF.0013 V0012906 CAT II TMF.0013

8500.2 IA Control: DCPP-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Noncompliance with DOD PPS requirements

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **TMF.0013**

Obtain The SSAA from the IAM. Examine the SSAA and the network interfaces listed. Ensure that the network ports, protocols, and services are listed for each
interface. Ensure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Refer to the firewall section and the packet filtering and logging section of the Network Checklist.
Ensure that enclaves have registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Default Finding Details The following issues were noted: System SSAA does not list the network ports, protocols, and services are for each application interface All System ports, protocols, and services are not registered in accordance with the DOD PPS. Enclave has not registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0013**

For applications:
Insure your SSAA lists all interfaces and the ports, protocols and services used for each
Insure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Notes:

TMF.0014 V0012907 CAT II TMF.0014

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section b.2.1

Vulnerability Removal of software services such as telnet, ftp, rsh, and rlogin if present is required for TMR Servers.

Vulnerability Discussion Any program that can be used to compromise the integrity of the TIVOLI enterprise are not to be installed on the TMR servers. Tivoli software frequently runs with elevated privileges and has a large span of control over hosts as a result any compromise of ESM elements could lead to widespread problems. Part of an attack might include disabling the ESM software so that security patches cannot be deployed, leaving a large number of hosts open to further attack

Checks **TMF.0014**

Have the IAM or the System Administrator issue a PS command to determine if telnet, ftp, rsh, and rlogin software services are actve or on the TMR server.

Default Finding Details The following software services were not removed from the TMR server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0014**

Prior to installing TMF software on a TMR server verify that telnet, ftp, rsh, and rlogin software services are not running on the system.

Notes:

TMF.0015 V0012908 CAT III TMF.0015

8500.2 IA Control: DCPR-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate Configuration Management (CM) process

Vulnerability Discussion Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without control of the system configuration. Unless the configuration is controlled by rigid processes administered by an independent board it is much less likely to be in an approved and accredited state.

Checks TMF.0015

Verify with the IAM that a CM process exists and it contains the following:
(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems (DCCB-1 and DCCB-2)
(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment (see also DCCT-1)
(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the
CM process are technically or procedurally not permitted.
Enhancements from NIST CM-3, Required for MAC 1 and Classified; Recommended for all others.
(1) The organization employs automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.
Note: This control requires a testing process; DCCT-1 requires the testing to be performed.

Default Finding Details The following CM issues were noted: There is no formal Configuration Management Process The CM process does not include formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation The CM process does not include a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems The CM process does not include a testing process to verify proposed configuration changes prior to implementation in the operational environment The CM process does not include a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted The organization does not employ automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0015

Implement a CM process that contains the following:
(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation
(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems (DCCB-1 and DCCB-2)
(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment (see also DCCT-1)
(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the
CM process are technically or procedurally not permitted.
Enhancements from NIST CM-3, Required for MAC 1 and Classified; Recommended for all others.
(1) The organization employs automated mechanisms to:
(i) document proposed changes to the information system;
(ii) notify appropriate approval authorities;
(iii) highlight approvals that have not been received in a timely manner;
(iv) inhibit change until necessary approvals are received; and
(v) document completed changes to the information system.

Notes:

TMF.0017 V0012909 CAT II TMF.0017

8500.2 IA Control: DCSP-1, PRNK-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Tivoli desktops are not located in an area, which is restricted from unauthorized access and protected by the local firewall.

Vulnerability Discussion The Tivoli Desktop is the standard graphical user interface (GUI) provided by Tivoli that enables administrators to communicate with the TMF and the other Tivoli products in the Tivoli Enterprise.Due to the capabilities to control the enterprise, these systems must be resticted to authorized users and protected .

Checks **TMF.0017**

Verify with the IAM and the Network Security Officer that Tivoli desktops are restricted from unauthorized access and are protected by a firewall.

Default Finding Details The TIVOLI desktop was not restricted to authorized user and was not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0017**

Make sure that TIVOLI Desktops are restricted to only authorized personnel and that they are located behind a firewall.

Notes:

TMF.0018 V0012910 CAT II TMF.0018

8500.2 IA Control: DCSP-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Access to Tivoli desktops is not restricted to policy regions.

Vulnerability Discussion A policy region is a logical collection of resources that are controlled by one or more policies. The set of managed resources that may exist in a policy region depends on the applications and the products installed in the TMR. Resource access is controlled when resources are organized in policy regions and authorization roles are assigned at the resource level. In this way Tivoli Desktops are limited to only those resources contained within the policy.

Checks **TMF.0018**

Have the TIVOLI Administrator show that the TIVOLI desktop is resticted by policy region.

Default Finding Details The following desktops were not limited to thier policy region.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0018**

The TIVOLI Administrator will establish poicy regions as part of the TIVOLI installation to control resources.

Notes:

TMF.0019 V0012911 CAT II TMF.0019

8500.2 IA Control: ECAN-1 References: Enterprise System Management STIG Section B.2.2

Vulnerability The Command Line Interface command was not resticted to authorized users.

Vulnerability Discussion The CLI enables an administrator to use Tivoli commands instead of navigating through the different panels of the Tivoli desktop. The CLI also provides administrators the ability to develop scripts that can be executed to perform management or administrative tasks in a single step. If not properly resticted it can enable users to control the TIVOLI Enterprise.

Checks **TMF.0019**

Ensure that the SA restricts CLI access to the TMR Administrator, the Policy Region Administrator(s), and IAM documented authorized personnel.

Default Finding Details The following users were not resticted from issuing the CLI command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0019**

Verify that CLI access is restricted to the TMR Administrator, the Policy Region Administrator(s), and IAM documented authorized personnel.

Notes:

TMF.0020 V0012913 CAT II TMF.0020

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.2.2.3

Vulnerability Inadequate access control mechanisms

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks **TMF.0020**

Verify with the IAM that access control mechanisms have been established and are working to ensure that all Tivoli servlets and support files are accessed and changed only by authorized personnel.

Default Finding Details Access control mechanisms do not exist to ensure that data is accessed and changed only by authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0020**

The IAM will verify that the system is configured to establish control mechanisms that ensure that data is accessed and changed only by authorized personnel.

Notes:

TMF.0022 V0012914 CAT II TMF.0022

8500.2 IA Control: ECTB-1 References: Enterprise System Management STIG Section B.2.2.3

Vulnerability The httpserv.log and the httptran.log files are not included as part of the regularly scheduled site backups.

Vulnerability Discussion Audit records provide the means for the IAO or other designated person to investigate any suspicious activity and to hold users accountable for their actions. If the records are not properly stored and protected, the IAO or other designated personnel will be able to unable to detect and investigate suspicious activity.

Checks **TMF.0022**

Verify with the IAO that the httpserv.log and the httptran.log files are backed up weekly and stored on different media.

Default Finding Details The httpserv.log and the httptran.log files are not are backed up weekly onto a different system or media than the system being audited.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0022**

Verify that the the httpserv.log and the httptran.log files are included on the list of weekly backup files.

Notes:

TMF.0024 V0012915 CAT II TMF.0024

8500.2 IA Control: ECPA-1 References: Enterprise System Management STIG Section B.2.3.1

Vulnerability Tivoli authorization roles were not used to restict Tivoli administrators granted root or privileged account authority on the systems they support from having system password or full root authority.

Vulnerability Discussion To perform many of the functions required by TIVOLI administrators on systems they support they require priveleged access. Tivoli requires that these administrators are be role based to reduce the access they are granted.

Checks **TMF.0024**

Review documentation to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Default Finding Details The following Issues were noted: Tivoli administrators were not broken into roles or security groups Individuals are not properly assigned to roles or security groups to limit thier access.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0024**

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment

Notes:

TMF.0025 V0012916 CAT I TMF.0025

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.3.1

Vulnerability Tivoli default accounts or passwords are not disabled.

Vulnerability Discussion Factory set, default or standard-user IDs and passwords were not removed or changed. This allows individuals familiar with these passwords to gain access to these systems.

Checks **TMF.0025**

Have the SA or TIVOLI administrator verfy that any default or installation set passwords were changed

Default Finding Details The following default passwords or user IDs were not changed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0025**

Have the TIVOLI Adminitrator validate that all factory set, default or standard-user IDs and passwords be removed or changed

Notes:

TMF.0026 V0012912 CAT II TMF.0026

8500.2 IA Control: ECPA-1 References: Enterprise System Management STIG Section B.2.3.2

Vulnerability Resource creation is not properly restricted.

Vulnerability Discussion In order for resources to be managed by Tivoli, they must be defined as managed resources. If creation of these resources are not properly resticted, than the abitily to control and assign them is copromised.

Checks **TMF.0026**

Verify with the IAM that creation of TIVOLI resources are resticted to only Tivoli administrators and authorized personnel.

Default Finding Details The following resources were not properly restricted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0026**

Verify with the IAM and TIVOLI administrator that TIVOLI resource creation is strictly controlled. Verify that a list of authorized TIIVOLI resources are maintained and updated.

Notes:

TMF.0027 V0012917 CAT II TMF.0027

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.3.3

Vulnerability TIVOLI policy creation and installation not limited to the TMR administrator and IAM documented authorized personnel

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information

Checks TMF.0027

Have the IAM ensure that policy creation and installation is limited to the TMR administrator and IAM documented authorized personnel only.

Default Finding Details Policy creation and installation was not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0027

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TMF.0028 V0012918 CAT II TMF.0028

8500.2 IA Control: ECPA-1 References: Enterprise System Management STIG Section B.2.3.3

Vulnerability The TMR administrator failed to properly restrict access at the policy region level and assigned resource rules.

Vulnerability Discussion Role based access allows for proper breakout of permissions and responsibilities for managing areas of responsibility. Properly restricting, assigning, and controlling these regions, allows for tighter control over the Tivoli enterprise.

Checks TMF.0028

Review documentation to ensure that system management privileges are broken into roles or security groups, and individuals are
assigned to these roles based on their job assignment.

Default Finding Details The following Issues were noted: System management privileges are not broken into roles or security groups Individuals are not properly assigned to roles or security groups

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0028

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Notes:

TMF.0029 V0012919 CAT II TMF.0029

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.3.4

Vulnerability Tivoli task creation and installation not restricted to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information

Checks **TMF.0029**

Have the IAM ensure that task creation and installation is restricted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details Task creation and installation was not restricted to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0029**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TMF.0030 V0012920 CAT II TMF.0030

8500.2 IA Control: CODB-1, CODB-2, CODB-3 References: Enterprise System Management STIG Section B.2.3.4

Vulnerability Task libraries are not backed up as part of the regularly scheduled backup process.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover

Checks **TMF.0030**

Validate that the procedures which detail that backups are to be performed at least weekly are implemented and the process is executed. Verify that the Tivoli task libraries are part of the sites backup procedures.

Default Finding Details Data backup is not performed at least weekly

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0030**

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed

Notes:

TMF.0031 V0012921 CAT II TMF.0031

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section B.2.3.5

Vulnerability Starting, stopping and configuration of the scheduler daemon is not being limited to the TMR administrator, and IAM documented authorized users

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TMF.0031

Verify that a least privilege policy controls access to the starting, stopping and configuration of the scheduler daemon and is limited to the TMR administrator, and IAM documented authorized personnel.

Default Finding Details The following issues were noted: The principle of least privilege is not being rigorously applied. The principle of separation of duties is not being enforced.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0031

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged accounts are not used for non-privileged functions

Notes:

TMF.0032 V0012922 CAT II TMF.0032

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.3.6

Vulnerability Notice group creation is not restricted to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion The information in notices is sesitive since it contains security violations and can be used as an audit trail. Creation of these groups must be resticted to preserve the integrity of the Tivoli region.

Checks TMF.0032

Verify with the IAO that notice group creation is restricted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details Notice group creation was not restricted to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0032

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0033 V0012923 CAT II TMF.0033

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section B.2.3.6

Vulnerability Notice group subscriptions are not restricted to the TMR administrator; the policy region administrators or IAM documented authorized personnel.

Vulnerability Discussion The information in notices is sensitive since it contains security violations and can be used as an audit trail. Creation of these groups must be resticted to preserve the integrity of the Tivoli region.

Checks TMF.033

Verify that a least privilege policy controls access to notice group subscriptions and are restricted to the TMR administrator; the policy region administrators or IAM documented authorized personnel.

Default Finding Details Notice group subscriptions are not restricted to the TMR administrator; the policy region administrators or IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.033

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms. Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged accounts are not used for non-privileged functions.

Notes:

TMF.0034 V0012924 CAT II TMF.0034

8500.2 IA Control: CODB-1, CODB-2, CODB-3 References: Enterprise System Management STIG Section B.2.3.6

Vulnerability Message catalogs are not backed up as part of the regularly scheduled backup process.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover

Checks TMF.0034

Validate that the procedures which detail that backups are to be performed at least weekly are implemented and the process is executed. Verify that the the message catalogs are backed up as part of the regularly scheduled backup process.

Default Finding Details Data backup is not performed at least weekly on the the message catalogs

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0034

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed

Notes:

TMF.0035 V0012925 CAT II TMF.0035

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG SEction B.2.3.7

Vulnerability The tnsnames.ora configuration file is not restricted from unauthorized access and update.

Vulnerability Discussion The tnsnames.ora configuration file is restricted from unauthorized access and updat. The RDBMS Interface Module (RIM) is responsible for providing a common interface between Tivoli application products and relational databases. RIM enables Tivoli application products to store and retrieve information in a database-independent manner.

Checks **TMF.0035**

Have the SA or TMR administrator ensure that the tnsnames.ora configuration file is restricted from unauthorized access and update.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **tmf.0035**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TMF.0036 V0012926 CAT II TMF.0036

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The Oracle instance ID specified in tnsnames.ora configuration file does not complie with instance names as specified in the Data Base STIG.

Vulnerability Discussion To avoid writing to the wrong database, the Oracle instance ID specified in tnsnames.ora configuration file complies with instance names as specified in the Data Base STIG.

Checks **TMF.0036**

Separated databases on the same host require strict partitioning of database datafiles, executables, and process/service host system resources. Labeling including file names, instance names, and other related variables must clearly distinguish the production and development
database resources in order to avoid any inadvertent access to the wrong database system. Database account names should differ between the two systems.
(DO0220: CAT IV) The DBA will not include a version number, Oracle-related or
otherwise, in production database instance names or Oracle SIDs.
(DO0220: CAT IV) The DBA will not use the default name of ORCL for production database
instance names or Oracle SIDs.

Default Finding Details the Oracle instance ID specified in tnsnames.ora configuration file does not comply with instance names as specified in the Data Base STIG

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0036**

The Tivoli Administrator will ensure the Oracle instance ID specified in tnsnames.ora configuration file complies with instance names as specified in the Data Base STIG.

Notes:

TMF.0037 V0012927 CAT II TMF.0037

8500.2 IA Control: DCPP-1 References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The port specified for SQL*Plus in tnsnames.ora configuration file does not comply with the approved ports as specified in DoDI 8551.1, (PPSM).

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **TMF.0037**

For applications:
Examine the SSAA and the network interfaces listed. Ensure that the network ports, protocols, and services are listed for each interface. Ensure that all ports, protocols, and services are registered in accordance with the DOD PPS.

Default Finding Details The port specified for SQL*Plus in tnsnames.ora configuration file does not comply with the approved ports as specified in DoDI 8551.1, (PPSM).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0037**

For applications:
Insure your SSAA lists all interfaces and the ports, protocols and services used for each
Insure that all ports, protocols, and services are registered in accordance with the DOD PPS.

Notes:

TMF.0038 V0012928 CAT II TMF.0038

8500.2 IA Control: DCPP-1 References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The communication protocol specified in the tnsnames.ora configuration file does not comply with the approved protocols as specified in DODI 8551.1, (PPSM).

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **TMF.0038**

For applications:
Examine the SSAA and the network interfaces listed. Ensure that the network ports, protocols, and services are listed for each interface. Ensure that all ports, protocols, and services are registered in accordance with the DOD PPS.

Default Finding Details The communication protocol specified in the tnsnames.ora configuration file does not comply with the approved protocols as specified in DODI 8551.1, (PPSM).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0038**

For applications:
Insure your SSAA lists all interfaces and the ports, protocols and services used for each Insure that all ports, protocols, and services are registered in accordance with the DOD PPS.

Notes:

TMF.0039 V0012929 CAT II TMF.0039

8500.2 IA Control: CODB-3, CODB-2, CODB-1 References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The Oracle database and audit log are not backed up as part of the regularly scheduled site backups.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover.

Checks TMF.0039

Validate With the SA that the procedures which detail that backups are to be performed at least weekly are implemented and the process is executed. Validate that the Tivoli Oracle database and audit log are backed up as part of the regularly scheduled site backups.

Default Finding Details Data backup is not performed for the Tivoli Oracle database and audit log.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0039

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed.

Notes:

TMF.0040 V0012930 CAT II TMF.0040

8500.2 IA Control: ECTP-1 References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The Oracle audit log isnot restricted from unauthorized access.

Vulnerability Discussion Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

Checks TMF.0040

Have the IAO verify that the SA, IAO and Tivoli administrators have access to read the audit log. The Tivoli administrator has the ability to delete the audit log after it is archived. No other access is permitted.

Default Finding Details Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0040

Verify that the SA, IAO and Tivoli administrators have access to read the audit log. The Tivoli administrator has the ability to delete the audit log after it is archived. No other access is permitted.

Notes:

TMF.0041 V0012931 CAT II TMF.0041

8500.2 IA Control: IAIA-2, IAIA-1

References: Enterprise System Management STIG Section B.2.3.7

Vulnerability The RIM APIs are not properly protected from unauthorized update and access.

Vulnerability Discussion Unauthorizrd access to the RIM APIs could be used to update the database and log datasets violating its integrity.

Checks **TMF.0041**

Have the IAM ensure that the RIM APIs are protected from unauthorized update and access.

Default Finding Details The RIM APIs were not properly protected from unathorized update and access.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0041**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TMF.0042 V0012932 CAT II TMF.0042

8500.2 IA Control: IAIA-1, IAIA-2

References: Enterprise System Management STIG Section B.2.4.1

Vulnerability Oserv service is not restricted from unauthorized access, update, starting and stopping.

Vulnerability Discussion The Object Dispatcher daemon, oserv, is responsible for coordinating communication between systems within a TME. Failure to restrict the access gives the controlling task control of the communications between the systems of the TME.

Checks **TMF.0042**

Have the IAO ensure the oserv service is restricted from unauthorized access, update, starting and stopping.

Default Finding Details The Object Dispatcher daemon, oserv service is not restricted from unauthorized access, update, starting and stopping

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0042**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0043 V0012933 CAT II TMF.0043

8500.2 IA Control: ECTP-1 References: Enterprise System Management STIG Section B.2.4.1 .

Vulnerability The TMR log file, $DBDIR/oservlog, is not restricted from unauthorized update and access.

Vulnerability Discussion Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

Checks **TMF.0043**

The IAO will restrict access to the TMR log file, $DBDIR/oservlog. Tivoli administrators are the only ones to have update or delete authorization to this file.

Default Finding Details The TMR log file, $DBDIR/oservlog, is not restricted from unauthorized update and access

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0043**

Verify that Tivoli administrators are the only ones to have update or delete authorization to this file.

Notes:

TMF.0045 V0012935 CAT II TMF.0045

8500.2 IA Control: CODB-1, CODB-2, CODB-3 References: Enterprise System Management STIG Section B.2.4.2

Vulnerability The TMF management database is not included as part of the regularly scheduled backup process.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recove

Checks **TMF.0045**

Validate that the procedures which detail that backups are to be performed at least weekly include the TMF management database.

Default Finding Details The TMF management database is not included as part of the regularly scheduled backup process

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0045**

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed.

Notes:

TMF.0046 V0012936 CAT II TMF.0046

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.4.3

Vulnerability The use of MDist is not limited to the TMR administrator and policy region administrator(s).

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0046**

The IAM will ensure the use of MDist is limited to the TMR administrator and policy region administrator(s).

Default Finding Details The use of MDist is not limited to the TMR administrator and policy region administrator(s).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0046**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0047 V0012937 CAT II TMF.0047

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.4.4

Vulnerability The use of SIS is not limited to the TMR Administrator and Policy Region Administrators.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0047**

The IAO will ensure the use of SIS is limited to the TMR Administrator and Policy Region Administrators only.

Default Finding Details The use of SIS is not limited to the TMR Administrator and Policy Region Administrators.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0047**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0048 V0012938 CAT II TMF.0048

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.4.5

Vulnerability The creation and installation of Tivoli Management Agent (TMA) is not limited to the TMR Administrator, and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0048

The IAO will ensure the creation and installation of TMAs is limited to the TMR Administrator, and IAM documented authorized personnel.

Default Finding Details The creation and installation of Tivoli Management Agent (TMA) is not limited to the TMR Administrator, and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0048

Implement the IA Control IAIA-. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0049 V0012939 CAT II TMF.0049

8500.2 IA Control: CODB-1, CODB-2, CODB-3 References: Enterprise System Management STIG Section B.2.4.5

Vulnerability The epmgrlog file is not included as part of the regularly scheduled backups.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover.

Checks TMF.0049

Validate that the procedures which detail that backups are to be performed at least weekly are implemented and the process is includes the epmgrlog file.

Default Finding Details The epmgrlog file is not included as part of the regularly scheduled backups.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0049

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed.

Notes:

TMF.0050 V0012940 CAT II TMF.0050

8500.2 IA Control: IAIA-2, IAIA-1 References: Enterprise System Management STIG Section B.2.4.6

Vulnerability Updates to the Tivoli Name Registry (TNR) are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information

Checks **TMF.0050**

The IAO will ensure updates to the TNR are limited to the TMR administrator and IAM documented authorized personnel

Default Finding Details Updates to the Tivoli Name Registry (TNR) are not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0050**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0051 V0012941 CAT III TMF.0051

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.4.7

Vulnerability The creation and maintenance of profiles and profile managers is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0051**

The IAO will ensure the creation and maintenance of profiles and profile managers is limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation and maintenance of profiles and profile managers is not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0051**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0052 V0012942 CAT II TMF.0052

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.5

Vulnerability The authorization of global TMR roles is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information

Checks **TMF.0052**

The IAO will ensure the authorization of global TMR roles is limited to the TMR administrator and IAM documented authorized personnel

Default Finding Details The authorization of global TMR roles is not limited to the TMR administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0052**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0053 V0012943 CAT II TMF.0053

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.5

Vulnerability The default Tivoli root administrator account or TMR administrator and a new Tivoli administrator root account, under a different name, is not crd assigning it to the eated.

Vulnerability Discussion By creating a new account that has root and assigning it to the Tivoli administrator and removing root privileges from the default account protects the default account from being able to have root access in the Tivoli enterprise and takes away the capabiity to violate the integrity of the systems in the enterprise.

Checks **TMF.0053**

The IAO will ensure the SA removes the default Tivoli root administrator account or TMR administrator and a new Tivoli administrator root account, under a different name, is created.

Default Finding Details The default Tivoli root administrator account or TMR administrator and a new Tivoli administrator root account, under a different name, was not created.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0053**

The SA should assign roles at the resource level. By assigning them to policy regions, the principle of least privilege is applied to Tivoli management and administration.

Notes:

TMF.0054 V0012944 CAT II TMF.0054

8500.2 IA Control: ECLP-1 References: Enterprise System Management STIG Section B.2.5

Vulnerability Tivoli administrators, who have been assigned administrative access to specific managed nodes, were provided administrative access to the TMR server from other Tivoli managed node.Separation of duties and least privilege principles not enforced

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TMF.0054

The IAM will ensure Tivoli administrators, assigned administrative access to specific managed nodes, are not provided administrative access to the TMR server from any Tivoli managed node.

Default Finding Details Tivoli administrators, who have been assigned administrative access to specific managed nodes, were provided administrative access to the TMR server from other Tivoli managed nodes

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0054

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged account is not used for non-privileged functio

Notes:

TMF.0055 V0012946 CAT II TMF.0055

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.6

Vulnerability Tivoli commands are not restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0055

The IAO will ensure Tivoli commands are restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

Default Finding Details Tivoli commands are not restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0055

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authenticationsystem (e.g., a unique token or user logon ID and password)

Notes:

TMF.0056 V0012947 CAT II TMF.0056

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.6

Vulnerability The use of Tivoli commands is not limited to IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0056**

The TMR administrator will ensure the use of Tivoli commands is limited to IAM documented authorized personnel.

Default Finding Details The use of Tivoli commands is not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0056**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0057 V0012948 CAT II TMF.0057

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.7

Vulnerability The installation of the Tivoli software to nonsupported platforms as documented by the vendor, is forbidden.

Vulnerability Discussion If sotware is impemented on non supported hardware, their is no record of testing on the platform and the integrity of the software has not been verified.

Checks **TMF.0057**

Have the Tivoli Administrator verify that the hardware being used for the Tivoli software is a suoorted system.

Default Finding Details The installation of the Tivoli software to nonsupported platforms as documented by the vendor, is forbidden.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0057**

Make sure that the system that is being used for Tivoli software is in the list of supported systems.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

TMF.0059 V0012950 CAT II TMF.0059

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.2.8

Vulnerability Tivoli directories are not properly restricted from unauthorized access and updates through file permissions or group authorizations.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks **TMF.0059**

Ensure that the SA restricts the Tivoli directories from unauthorized access and updates through file permissions or group authorizations.

Default Finding Details Tivoli directories are not properly restricted from unauthorized access and updates through file permissions or group authorizations

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0059**

The system should establish control mechanisms to ensure that data is accessed and changed only by authorized personnel.

Notes:

TMF.0060 V0012951 CAT II TMF.0060

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.8

Vulnerability Tivoli install files were not removed from the system upon successful completion of the installation process.

Vulnerability Discussion Tivoli install files must be removed or protected from access from everyone with the exception of the Tivoli administrator, to avoid any unsecured access to any of the TIVOLI products that could be used to violate the integrity of the TIVOLI enterprise.

Checks **TMF.0060**

The Tivoli administrator must verify that all installation files and libraries are removed or properly protected.

Default Finding Details After completing the install of Tivoli, all install files and libraies were not protected or removed from the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0060**

The SA will ensure that all files related to TIVOLI install are remove or the use is restricted to the TIVOLI administrator.

Notes:

TMF.0061 V0012952 CAT II TMF.0061

8500.2 IA Control: ECAN-1, ECPA-1 References: Enterprise System Management STIG Section B.2.9

Vulnerability The assignment of roles necessary to update and access resources of interconnected TMRs are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to restrict access to classified or sensitive data to authorized personnel violates the integrity and privacy of that information.

Checks **TMF.0061**

The IAO will ensure the assignment of roles necessary to update and access resources of interconnected TMRs are limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The following issues were noted: Access to classified or sensitive data is granted without verifying need-to-know Access is not enforced by discretionary or role-based access controls Proper audit of access is not performed

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0061**

Develop, implement and enforce procedure to insure that the need to know is established before access is granted to classified or sensitive data. Develop and implement discretionary or role-based access controls.
Ensure proper auditing is performed of both access and attempted access and insure proper audit records are created

Notes:

TMF.0062 V0012953 CAT II TMF.0062

8500.2 IA Control: DCNR-1 References: Enterprise System Management STIG Section B.2.10

Vulnerability NIST FIPS 140-2 validated cryptography is not used to implement encryption

Vulnerability Discussion Approved algorithms are necessary to prevent compromise and theft of data.

Checks **TMF.0062**

The IAM will ensure NIST FIPS 140-2 validated cryptography is used to implement encryption.

Default Finding Details Functions of the application and the enclave (network) that implement encryption, digital signature, key exchange and/or hash use algorithms that are not FIPS 140-2 compliant

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0062**

Ensure the algorithms are FIPS 140-2 compliant by checking the NIST web site (www.nist.gov). Replace or upgrade systems that do not use approved algorithms.

Notes:

TMF.0063 V0012954 CAT II TMF.0063

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.11.1

Vulnerability Access and use of the Tivoli AEF to IAM documented authorized personnel was not restricted.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0063**

Verify that TMR administrator restricted access and use of the Tivoli AEF to IAM documented authorized personnel if the AEF was used.

Default Finding Details Access and use of the Tivoli AEF to IAM documented authorized personnel was not restricted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0063**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0064 V0012955 CAT II TMF.0064

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.11.1

Vulnerability All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0064

The IAO will ensure all installations and updates to the Tivoli AEF are restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Default Finding Details All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0064

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0065 V0012956 CAT II TMF.0065

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.11.2

Vulnerability Access and use of the Tivoli EIF to IAM documented authorized personnel was not properly restricted.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0065

Verify that the TMR administrator restricted access and use of the Tivoli EIF to IAM documented authorized personnel.

Default Finding Details Access and use of the Tivoli EIF to IAM documented authorized personnel was not properly restricted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0065

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0066 V0012957 CAT II TMF.0066

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG SEction B.2.11.2

Vulnerability All installations and updates to the Tivoli EIF were not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0066

Ensure that the TMR administrator limited access and use of the Tivoli ADE to IAM documented authorized personnel.

Default Finding Details All installations and updates to the Tivoli EIF were not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0066

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0067 V0012958 CAT II TMF.0067

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.11.3

Vulnerability Access and use of the Tivoli Application Development Environment (ADE) was not limited to IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0067

Verify that the TMR administrator limited access and use of the Tivoli ADE to IAM documented authorized personnel.

Default Finding Details Access and use of the Tivoli ADE was not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0067

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMF.0068 V0012959 CAT II TMF.0068

8500.2 IA Control: IAIA-1, IAIA-2

References: Enterprise System Management STIG Section B.2.11.3

Vulnerability All installations and updates to the Tivoli Application Development Environment (ADE) are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0068**

The IAO will ensure all installations and updates to the Tivoli ADE are restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Default Finding Details All installations and updates to the Tivoli ADE are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0068**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

9. CHECKLIST INSTRUCTIONS – Tivoli Enterprise Console Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Enterprise Console Checks that must be reviewed if reviewing Tivoli Enterprise Console. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

TEC.0002 V0012964 CAT II TEC.0002

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.3.1

Vulnerability The TEC product was not installed using the TMF SIS or approved vendor-supplied scripts.

Vulnerability Discussion The only valid installation of TIVOLI products is via SIS or approved Vendor scripts. Failure to utilize these two methods could impact the integrity of the Tivoli Enterprise.

Checks **TEC.0002**

The TMR administrator and SA will ensure that TMF SIS or approved vendor-supplied scripts were used to install the TEC product..

Default Finding Details The TEC product was not installed using the TMF SIS or approved vendor-supplied scripts.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0002**

The Tivoli Administrator will ensure that TMF SIS or approved vendor-supplied scriptsare only used to install Tivoli Prodcts.

Notes:

TEC.0009 V0012960 CAT III TEC.0009

8500.2 IA Control: CODP-1, CODP-2, CODP-3 References: Enterprise System Management STIG Section B.3.1

Vulnerability A contingency processing plan does not exists for the TEC servers, database, applications and adapters in the TME.

Vulnerability Discussion Well thought out recovery plans are essential for system recovery and/or business restoral in the event of catastrophic failure or disaster

Checks **TEC.0009**

The IAM will ensure a contingency processing plan exists for the TEC servers, database, applications and adapters in the TME.

Default Finding Details A contingency processing plan does not exists for the TEC servers, database, applications and adapters in the TME.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0009**

Develop a Disaster Recovery Plan for the Information System or Facility Insure the plan: provides for partial resumption of function within 5 days contains business recovery plans
contains system contingency plans contains facility disaster recovery plans is officially accepted by the IS or facility owner

Notes:

TEC.0010 V0012962 CAT II TEC.0010

8500.2 IA Control: CODB-1, CODB-2, CODB-3 References: Enterprise System Management STIG Section B.3.1

Vulnerability The TEC event database and server files are not backed up as part of the regularly scheduled backup process.

Vulnerability Discussion If backups are not properly processed, recovery of system failure or implementation of a contingency plan would not include the data necessary to fully recover.

Checks TEC.0010

The SA and TMR administrator will ensure the TEC event database and server files are backed up as part of the regularly scheduled backup process.

Default Finding Details The TEC event database and server files are not backed up as part of the regularly scheduled backup process.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0010

Implement procedures which detail that backups are to be performed at least weekly and insure the process is properly executed.

Notes:

TEC.0011 V0012905 CAT II TEC.0011

8500.2 IA Control: COTR-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate Recovery Procedures

Vulnerability Discussion Improper system recovery can result in loss or compromise of sensitive information and/or compromise of the system by unauthorized individuals who seize the opportunity to exploit known vulnerabilities. Tivoli requires a trusted recovery of the TMR, policy regions, managed nodes and gateways in the event of a technical failure.

Checks TEC.0011

The TMR administrator, TEC administrator and Tivoli administrators will maintain documentation as part of the disaster recovery plan describing the procedures necessary to perform a trusted recovery of the TEC to include the event server, database, adapter files, software and configuration files.

Default Finding Details The following issues were noted: Recovery procedures and technical system features do not exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are not documented. Circumstances that can inhibit trusted recover are documented but appropriate mitigating procedures are not in place. There is no list of personnel authorized to perform the recover function.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0012

Insure that the DRP or SOP has recovery procedures that indicate the steps needed for secure recovery. Verification process can include original COTS or GOTS installation media or a hash of the installation program. These procedures should include any special considerations for trusted recovery such as network attachment or placement. The procedure should also include the list of authorized personnel that perform the function.

Notes:

TEC.0012 V0012965 CAT II TEC.0012

8500.2 IA Control: ECAN-1, ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.2.1

Vulnerability Authorizations and permissions necessary for the creation, distribution and implementation of TME endpoint adapters, TME managed node adapters, and non-TME adapters are not limited to the TMR administrator, the TEC administrator and IAM documented authorized personnel.

Vulnerability Discussion The following issues were noted: Access to classified or sensitive data is granted without verifying need-to-know Access is not enforced by discretionary or role-based access controls Proper audit of access is not performed

Checks TEC.0012

Have the IAM will ensure the roles, authorizations and permissions necessary for the creation, distribution and implementation of TME endpoint adapters, TME managed node adapters, and non-TME adapters are limited to the TMR administrator, the TEC administrator and IAM documented authorized personnel.

Default Finding Details Authorizations and permissions necessary for the creation, distribution and implementation of TME endpoint adapters, TME managed node adapters, and non-TME adapters are not limited to the TMR administrator, the TEC administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0012

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Notes:

TEC.0017 V0012968 CAT II TEC.0017

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.3.2.3

Vulnerability All TEC web console access via platform access security authorizations and web server security manager policies is not being enforced.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information. Faiure to secure the communications between the web consoles and WAS could open up the enterprise to a Man-in-the-Middle attack.

Checks TEC.0017

Have the IAM and Web Administrator ensure that access to the event consoles is controlled through platform security and roles assigned to the administrator or operator.

Default Finding Details All TEC web console access via platform access security authorizations and web server security manager policies is not being enforced.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0017

The IAM will ensure that all TEC web console access is secured through the platforms security and that policies exist restricting access to the administrator and operator only.

Notes:

TEC.0022 V0013001 CAT II TEC.0022

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.3.2.4

Vulnerability Access and updates of the UI server filesare not limited to IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TEC.0022

Ensure that the SA, TMR administrator, and TEC administrator limits access and updates of the UI server files to IAM documented authorized personnel.

Default Finding Details Access and updates of the UI server filesare not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0022

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TEC.0023 V0013004 CAT II TEC.0023

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.3.2.4

Vulnerability Usage of UI server commands is not limited to the TEC administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TEC.0023

Ensure that the SA and TMR administrator restricts usage of UI server commands to the TEC administrator and IAM documented authorized personnel.

Default Finding Details Usage of UI server commands is not limited to the TEC administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0023

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TEC.0025 V0013005 CAT II TEC.0025

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.2.5

Vulnerability Access to the ACF, use of the NetView Web Console, and NetView Native console was not properly restricted via platform security requirements and Tivoli roles.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation

Checks TEC.0025

Ensure that the TMR administrator, TEC administrator and SA restricts access to the ACF, the NetView Web Console, and the NetView Native console via platform security requirements and Tivoli roles.

Default Finding Details Access to the ACF, use of the NetView Web Console, and NetView Native console was not properly restricted via platform security requirements and Tivoli roles.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0025

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TEC.0026 V0013006 CAT II TEC.0026

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.2.5

Vulnerability Creation, distribution and installation of profiles are not limited to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TEC.0026

Ensure that the TMR administrator limits the creation, distribution and installation of profiles to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.

Default Finding Details Creation, distribution and installation of profiles are not limited to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0026

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TEC.0033 V0013007 CAT II TEC.0033

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.2.9

Vulnerability ARF file creation, maintenance, and implementation via authorization roles is not limited to IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks **TEC.0033**

Ensure that the TMR administrator and the SA will limit ARF file creation, maintenance, and implementation via authorization roles to IAM documented authorized personnel.

Default Finding Details ARF file creation, maintenance, and implementation via authorization roles is not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0033**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TEC.0036 V0013008 CAT II TEC.0036

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.3

Vulnerability RIM authorization roles are not limited to the TEC administrator and IAM documented authorized personnel.

Vulnerability Discussion The following Issues were noted: System management privileges are not broken into roles or security groups Individuals are not properly assigned to roles or security groups

Checks **TEC.0036**

Have the IAO ensure RIM authorization roles are limited to the TEC administrator and IAM documented authorized personnel.

Default Finding Details RIM authorization roles are not limited to the TEC administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0036**

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Notes:

TEC.0038 V0013009 CAT II TEC.0038

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.4

Vulnerability Access and updates to Tivoli Enterprise Console gateway files is not restricted to IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TEC.0038

Ensure that the SA and the TMR administrator restrict access and updates to Tivoli Enterprise Console gateway files to IAM documented authorized personnel.

Default Finding Details Access and updates to Tivoli Enterprise Console gateway files is not restricted to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0038

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions

Notes:

TEC.0041 V0013010 CAT II TEC.0041

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.5

Vulnerability The authorization of TEC roles is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TEC,0041

Verify that the IAO ensures the authorization of TEC roles is limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The authorization of TEC roles is not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0041

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions

Notes:

TEC.0044 V0013011 CAT II TEC.0044

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.6

Vulnerability The distribution of adapters and event class files is not limited to the TMR Administrator, and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TEC.0044

Have the IAOl ensure the distribution of adapters and event class files are limited to the TMR Administrator, and IAM documented authorized personnel.

Default Finding Details The distribution of adapters and event class files is not limited to the TMR Administrator, and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0044

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that they do not use their privileged account for non-privileged functions.

Notes:

TEC.0046 V0013012 CAT II TEC.0046

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.3.7.1

Vulnerability Use of the wrb commands is not restricted to the TMR administrator, TEC administrator, and IAM documented authorized personnel via file permissions and Tivoli authorization roles.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TEC.0046

Verify that the SA and TMR administrator restricts the use of the wrb commands to the TMR administrator, TEC administrator, and IAM documented authorized personnel via file permissions and Tivoli authorization roles

Default Finding Details Use of the wrb commands is not restricted to the TMR administrator, TEC administrator, and IAM documented authorized personnel via file permissions and Tivoli authorization roles.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0046

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TEC.0047 V0013013 CAT II TEC.0047

8500.2 IA Control: ECLP-1, IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.3.7.1

Vulnerability Rule base creation and distribution was not restricted to the TEC administrator and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been

Checks **TEC.0047**

Ensure that the TMR administrator restricts rule base creation and distribution to the TEC administrator and IAM documented authorized personnel

Default Finding Details Rule base creation and distribution was not restricted to the TEC administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0047**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TEC.0048 V0013014 CAT II TEC.0048

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.3.7.1

Vulnerability Rule base target directory permissions are not restricted in accordance with the Object Permissions section of the ESM TIVOLI STIG.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, and customer data.

Checks **TEC.0048**

Verify that the IAM ensures the SA and TMR administrator have restricted rule base target directory permissions in accordance with the Object Permissions section of the ESM Tivoli STIG.

Default Finding Details Rule base target directory permissions are not restricted in accordance with the Object Permissions section of the ESM TIVOLI STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TEC.0048**

Insure proper DACLs are in place for directories and files that contain system binaries.

Notes:

TEC.0059 V0013015 CAT II TEC.0059

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.3.10

Vulnerability Access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems are not restricted in accordance with the Object Permissions specified in the ESM Tivoli STIG.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, and customer data.

Checks TEC.0059

Ensure that the SA restricts access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems in accordance with the Object Permissions section of the ESM Tivoli STIG.

Default Finding Details Access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems are not restricted in accordance with the Object Permissions specified in the ESM Tivoli STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0059

Insure proper DACLs are in place for directories and files that contain system binaries

Notes:

TEC.0060 V0013016 CAT II TEC.0060

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.3.10

Vulnerability Access to the TEC adapter files is not restricted in accordance with the Object Permissions section of the ESM Tivoli STIG.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, and customer data.

Checks TEC.0060

Ensure thatThe SA restricts access to the TEC adapter files in accordance with the Object Permissions section.

Default Finding Details Access to the TEC adapter files is not restricted in accordance with the Object Permissions section of the ESM Tivoli STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TEC.0060

Insure proper DACLs are in place for directories and files that contain system binaries.

Notes:

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks TME.0001

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TME.0001

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0007 V0012900 CAT II TMF.0007

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.1

Vulnerability Systems hosting TIVOLI Sostware will be configured as specified in the ESM STIG.

Vulnerability Discussion Due to the capabilities of TIVOLI software to alter information on the systems it controls. It is important to properly secure the TIVOLI software.

Checks TMF.0007

Verify with the IAM that the Tivoli software was installed following the configuration specified in the ESM STIG and the STIG of the system it was installed on. If installed on WINDOWS or UNIX systems, verify that physical security of the platforms, network connectivity, file access controls, change management and backups and recovery be addressed so as to ensure the confidentiality, availability and integrity of the Tivoli Enterprise and the resources that exist in it.

Default Finding Details The following TIVOLI Managegment software was not configued as specified in the ESM STIG and the STIG of the system it was installed on.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0007

When installing TIVOLI software validate that it is configred as specified in the ESM STIG and the STIG of the system it was installed on.

Notes:

TMF.0009 V0012902 CAT III TMF.0009

8500.2 IA Control: DCCT-1 References: Enterprise System Management STIG Section B.2.1

Vulnerability Inadequate Deployment Procedures

Vulnerability Discussion Undocumented procedures for upgrading or deploying new hardware, software or software upgrades for Tivoli systems can lead to inconsistent deployments which can cause incompatibility problems between devices and systems and/or possible security holes. These problems or holes can lead to slowdowns or outages on the network or unauthorized access or attacks on DoD assets.

Checks **TMF.0009**

The IAO will Ensure procedures exist which address the testing and implementation process for all patches, upgrades and AIS deployments.
The procedures should be in the Configuration Management Plan.
For Lab tested systems ensure the PM details the testing and release process and addresses change control in the PM's deployment plan.

Default Finding Details Procedures which address the testing and implementation process for all patches, upgrades and AIS deployments do not exist

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0009**

The IAO will ensure that procedures are documented in the configuration Management Plan.

Notes:

TMF.0010 V0012903 CAT III TMF.0010

8500.2 IA Control: CODP-2 References: Enterprise System Management STIG Section b.2.1

Vulnerability Inadequate Disaster Recovery Plan

Vulnerability Discussion Disaster Recovery Plan does not allow for the resumption of mission or business critical functions within 24 hours.

Checks **TMF.0010**

The IAM will ensure that a written plan exists that addresses the partial resumption of mission or business essential functions with 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Default Finding Details Well thought out recovery plans are essential for system recovery and/or business restoral in the event of catastrophic failure or disaster.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0010**

The Tivoli administrator must Develop a Disaster Recovery Plan for the Information System or Facility that Insures the plan:
provides for partial resumption of function within 24 hours
contains business recovery plans
contains system contingency plans
contains facility disaster recovery plans
is officially accepted by the IS or facility owner

Notes:

TMF.0013 V0012906 CAT II TMF.0013

8500.2 IA Control: DCPP-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Noncompliance with DOD PPS requirements

Vulnerability Discussion Failure to comply with DoD ports, protocols, and services (PPS) requirements can result in compromise of enclave boundary protections and/or functionality of the AIS.

Checks **TMF.0013**

Obtain The SSAA from the IAM. Examine the SSAA and the network interfaces listed. Ensure that the network ports, protocols, and services are listed for each
interface. Ensure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Refer to the firewall section and the packet filtering and logging section of the Network Checklist.
Ensure that enclaves have registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Default Finding Details The following issues were noted: System SSAA does not list the network ports, protocols, and services are for each application interface All System ports, protocols, and services are not registered in accordance with the DOD PPS. Enclave has not registered all active ports, protocols, and services in accordance with DoD and DoD Component guidance

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0013**

For applications:
Insure your SSAA lists all interfaces and the ports, protocols and services used for each
Insure that all ports, protocols, and services are registered in accordance with the DOD PPS.
For Lab tested systems ensure this information is addressed in the PM's deployment plan for the hosting enclave. (See DCID-1)
For Enclaves:
Register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

TMF.0064 V0012955 CAT II TMF.0064

8500.2 IA Control: IAIA-1, IAIA-2

References: Enterprise System Management STIG Section B.2.11.1

Vulnerability All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMF.0064

The IAO will ensure all installations and updates to the Tivoli AEF are restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Default Finding Details All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0064

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

10. CHECKLIST INSTRUCTIONS – Tivoli Monitoring Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Monitoring Checks that must be reviewed if reviewing Tivoli Monitoring. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

TIM.0007 V0013017 CAT II TIM.0007

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.4.1

Vulnerability The creation, distribution and implementation of Tivoli Monitoring endpoint monitors or resource models are not restricted to TMR administrators and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TIM.0007**

Verify that the IAO ensures the creation, distribution and implementation of Tivoli Monitoring endpoint monitors or resource models are restricted to TMR administrators and IAM documented authorized personnel

Default Finding Details The creation, distribution and implementation of Tivoli Monitoring endpoint monitors or resource models are not restricted to TMR administrators and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0007**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TIM.0009 V0013018 CAT II TIM.0009

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.4.2.2

Vulnerability The Web Health Consoles are not installed on a platform that is secured in accordance with the appropriate platform STIGs.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks **TIM.0009**

Verify that the IAO ensures the Web Health Consoles are installed on a platform that is secured in accordance with the appropriate platform STIGs.

Default Finding Details The Web Health Consoles are not installed on a platform that is secured in accordance with the appropriate platform STIGs.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0009**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TIM.0014 V0013019 CAT II TIM.0014

8500.2 IA Control: DCCS-1, DCCS-2

References: Enterprise System Management STIG Section B.4.2.2

Vulnerability All security requirements for Internet browsers are not implemented in accordance with the Desktop Application STIG.

Vulnerability Discussion Failure to use approved configuration guidance does not assure that the system is initially free of security issues inherent in newly deployed IA and IA enabled products.

Checks **TIM.0014**

The SA will implement all security requirements for Internet browsers in accordance with the Desktop Application STIG.

Default Finding Details The organization does not use A DoD reference document, such as a security technical implementation guide (STIG) or security recommendation guide as the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products. This may leave the systems vulnerable to attack.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0014**

Use A DoD reference document, such as a security technical implementation guide (STIG) or security recommendation guide as the primary source for security configuration or implementation guidance for the deployment IA- and IA-enabled IT products. If a DoD reference document is not available, work with DISA or NSA to draft configuration guidance for inclusion in a Departmental
reference guide.

Notes:

TIM.0015 V0013020 CAT II TIM.0015

8500.2 IA Control: DCCS-1, DCCS-2

References: Guide to Secure Configuration and Administration of Microsoft SQL Server 2000 Section B.4.2.2

Vulnerability The WebSphere Application Server is not secured in accordance with the Web Server and platform STIGs.

Vulnerability Discussion Failure to follow the configuration of the Web Server STIG, wil make it easy for malicious users to gather information about the configuration of the web server.

Checks TIM.0015

The IAO will ensure the WebSphere Application Server is secured in accordance with the Web Server and platform STIGs. to check the following vulnerabilities.

(WG135: CAT II) The Web Manager or SA will ensure that unnecessary services are disabled from the web server, except those that are expressly permitted.
• (WN010: CAT II) The Web Manager will ensure the termination timeout (or equivalent parameter) is set to one second or less.
• (WA170: CAT II) The IAO will ensure that procedures are in place that require the SA or Web Manager to investigate any unscheduled or unanticipated disruption to the web service (i.e, this will normally involve a thorough review of the appropriate logs).
• (WG110: CAT II) The Web Manager will ensure the number of simultaneous requests that a web server allows is not set to unlimited.
• (WG520: CAT II) The Web Manager or SA will ensure the advertising of information pertaining to the operating system version, web server type and version, and web server ports is restricted.
• (WN020: CAT II) The Web Manager will ensure that in the case of Netscape, automatic directory indexing is turned off.
Web Server STIG, V5R1 DISA Field Security Operations
29 October 2004 Developed by DISA for the DOD
UNCLASSIFIED
13
• (WG170: CAT II) The Web Manager will ensure the web server is configured such that a user cannot traverse from a document directory to a directory that does not contain web content.
• (WG170: CAT II) The Web Manager will ensure that each readable web document directory contains a default, home, index, or equivalent file.

Default Finding Details The WebSphere Application Server is not secured in accordance with the Web Server and platform STIGs.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TIM.0015

Use A DoD reference document, such as a security technical implementation guide (STIG) or security recommendation guide as the primary source for security configuration or implementation guidance for the deployment IA- and IA-enabled IT products. If a DoD reference document is not available, work with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.

Notes:

TIM.0016 V0013021 CAT II TIM.0016

8500.2 IA Control: DCSL-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE Section B.4.2.3

Vulnerability The endpoint component software is not restricted in accordance with the minimal guidelines as specified in the Object Permissions section of the ESM Tivoli STIG.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, and customer data.

Checks TIM.0016

The SA will restrict the endpoint component software in accordance with the minimal guidelines as specified in the Object Permissions section.

Default Finding Details The endpoint component software is not restricted in accordance with the minimal guidelines as specified in the Object Permissions section of the ESM Tivoli STIG

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TIM.0016

Insure proper DACLs are in place for directories and files that contain system binaries

Notes:

TIM.0017 V0013022 CAT II TIM.0017

8500.2 IA Control: ECLP-1, ECPA-1

References: Enterprise System Management STIG Section B.4.2.4

Vulnerability Heartbeat configuration updates (A process that creates an audit log for each remote session) is not limited to IAM documented authorized personnel.
.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TIM.0017

Ensure that the TMR administrator limits heartbeat configuration updates to IAM documented authorized personnel.

Default Finding Details Heartbeat configuration updates (A process that creates an audit log for each remote session) is not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TIM.0017

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TIM.0018 V0013023 CAT II TIM.0018

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.4.2.4

Vulnerability The TMR administrator did not limit access to the heartbeat configuration updates to Tivoli Monitoring Notice Group.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks **TIM.0018**

Ensure that the TMR administrator limits access to the heartbeat configuration updates to the Tivoli Monitoring Notice Group.

Default Finding Details The TMR administrator did not limit access to the heartbeat configuration updates to Tivoli Monitoring Notice Group.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0018**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TIM.0019 V0013024 CAT II TIM.0019

8500.2 IA Control: ECTP-1 References: Enterprise System Management STIG Section B.4.2.5

Vulnerability The Gathering Historical database from is not restricted from unnauthorized access update.

Vulnerability Discussion Excessive permissions of audit records allow cover up of intrusion or misuse of the application.

Checks **TIM.0019**

Ensure that the SA restricts the Gathering Historical database from unauthorized access update

Default Finding Details The Gathering Historical database from is not restricted from unnauthorized access update

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0019**

Implement the following controls on audit records:
SA can read audit logs IAO are authorized to delete the audit log after it is archived
No other access is permitted.

Notes:

TIM.0021 V0013025 CAT II TIM.0021

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.4.2.6

Vulnerability ETL script creation and implementation is not restricted to IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks **TIM.0021**

Ensure that the TMR administrator and SA restricts ETL script creation and implementation to IAM documented authorized personnel.

Default Finding Details ETL script creation and implementation is not restricted to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0021**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TIM.0026 V0013026 CAT III TIM.0026 (TMF.0026)

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.4.5

Vulnerability The creation and maintenance resource models are not restricted to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks **TIM.0026**

Verify that the IAO ensures the creation and maintenance resource models are restricted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation and maintenance resource models are not restricted to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TIM.0026**

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TIM.0027 V0013027 CAT II TIM.0027

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.4.6

Vulnerability The Tivoli Monitoring commands are not restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TIM.0027

Verify that the IAO ensures the Tivoli Monitoring commands are restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

Default Finding Details The Tivoli Monitoring commands are not restricted from unauthorized access and usage through the assignment of permissions or group authorizations.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TIM.0027

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks TME.0001

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TME.0001

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0003 V0012779 CAT II TMF.0003

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.2.1

Vulnerability TMF software not being protected from unauthorized use.

Vulnerability Discussion The TMF software is very powerful and must be protected from unathorized use, to avoid attacks on other systems or introduction of unathorized code.

Checks **TMF.0003**

Have the IAO verify that all software modules and libraries are restricted to ESM authorized users

Default Finding Details The following software libraries were not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0003**

Have the IAO validate that all libraries containing TMF modules are properly protected and open only to authorized users.

Notes:

TMF.0017 V0012909 CAT II TMF.0017

8500.2 IA Control: DCSP-1, PRNK-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Tivoli desktops are not located in an area, which is restricted from unauthorized access and protected by the local firewall.

Vulnerability Discussion The Tivoli Desktop is the standard graphical user interface (GUI) provided by Tivoli that enables administrators to communicate with the TMF and the other Tivoli products in the Tivoli Enterprise.Due to the capabilities to control the enterprise, these systems must be resticted to authorized users and protected .

Checks **TMF.0017**

Verify with the IAM and the Network Security Officer that Tivoli desktops are restricted from unauthorized access and are protected by a firewall.

Default Finding Details The TIVOLI desktop was not restricted to authorized user and was not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0017**

Make sure that TIVOLI Desktops are restricted to only authorized personnel and that they are located behind a firewall.

Notes:

TMF.0018 V0012910 CAT II TMF.0018

8500.2 IA Control: DCSP-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Access to Tivoli desktops is not restricted to policy regions.

Vulnerability Discussion A policy region is a logical collection of resources that are controlled by one or more policies. The set of managed resources that may exist in a policy region depends on the applications and the products installed in the TMR. Resource access is controlled when resources are organized in policy regions and authorization roles are assigned at the resource level. In this way Tivoli Desktops are limited to only those resources contained within the policy.

Checks **TMF.0018**

Have the TIVOLI Administrator show that the TIVOLI desktop is resticted by policy region.

Default Finding Details The following desktops were not limited to thier policy region.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0018**

The TIVOLI Administrator will establish poicy regions as part of the TIVOLI installation to control resources.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

11. CHECKLIST INSTRUCTIONS – Tivoli Configuration Manager Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Configuration Manager Checks that must be reviewed if reviewing Tivoli Configuration Manager. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

TCM.0007 V0012970 CAT II TCM.0007

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.5.2.1

Vulnerability The roles, authorizations and permissions necessary for the creation, distribution and implementation of software packages to IAM documented authorized personnel were not limited.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TCM.0007

ensure with the TMR administrator that the roles, authorizations and permissions necessary for the creation, distribution and implementation of software packages are limited to IAM documented authorized personnel

Default Finding Details The roles, authorizations and permissions necessary for the creation, distribution and implementation of software packages to IAM documented authorized personnel were not limited.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMC.0007

Establish and enforce a least privilege policy that controls
the roles, authorizations and permissions necessary for the creation, distribution and implementation of software packages. Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged accounts are not used for non-privileged functions

Notes:

TCM.0008 V0012971 CAT II TCM.0008

8500.2 IA Control: ECLP-1, ECPA-1, IAIA-1 References: Enterprise System Management STIG Section B.5.2.1

Vulnerability Access and update authority of the Software Package Editor was not limited to IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TCM.0008

Verify with the TMR administrator that access and update authority of the Software Package Editor has been restricted to authorized personnel.

Default Finding Details Access and update authority of the Software Package Editor was not limited to IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0008

Implement and enforce procedures to ensure that system management privileges are broken into roles or security groups, and individuals are assigned to these roles based on their job assignment.

Notes:

TCM.0009 V0012972 CAT II TCM.0009

8500.2 IA Control: IAIA-2, IAIA-1 References: Enterprise System Management STIG Section B.5.2.2

Vulnerability The creation and maintenance of inventory profiles and profile managers is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TCM.0009

Have the IAO ensure that the creation and maintenance of inventory profiles and profile managers is restricted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation and maintenance of inventory profiles and profile managers is not limited to the TMR administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0009

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TCM.0010 V0012973 CAT II TCM.0010

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.5.2.3

Vulnerability The creation and maintenance of activity plans is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TCM.0010

Ensure that the IAO restricts the creation and maintenance of activity plans to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation and maintenance of activity plans is not limited to the TMR administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0010

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password).

Notes:

TCM.0011 V0012974 CAT II TCM.0011

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.5.2.3

Vulnerability Access to the Activity Planner administrative interface is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TCM.0011

Have the IAO ensure that access to the Activity Planner administrative interface is resticted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details Access to the Activity Planner administrative interface is not limited to the TMR administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0011

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged accounts are not used for non-privileged functions

Notes:

TCM.0012 V0012975 CAT IV TCM.0012

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.5.2.3

Vulnerability Access to the Activity Planner commands is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TCM.0012

Have the IAO ensure access to the Activity Planner commands is resticted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details Access to the Activity Planner commands is not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0012

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that their privileged accounts are not used for non-privileged functions

Notes:

TCM.0014 V0012977 CAT II TCM.0014

8500.2 IA Control: ECLP-1, ECPA-1 References: Enterprise System Management STIG Section B.5.2.5

Vulnerability Pervasive device access to the IBM Tivoli Configuration Manager is not limited to IAM documented authorized personnel.

Vulnerability Discussion Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system. Also, If a hacker gains access to an account they assume the privileges of the user; Minimizing privileges reduces the risk associated with hijacked accounts. Using a privileged account to perform routine functions makes the computer vulnerable to attack by any virus or Trojan Horse inadvertently introduced during a session that has been granted full privileges. The rules of least privilege and separation of duties must always be enforced.

Checks TCM.0014

Ensure that the IAO limits pervasive device access to the IBM Tivoli Configuration Manager and IAM documented authorized personnel.

Default Finding Details Pervasive device access to the IBM Tivoli Configuration Manager is not limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0014

Establish and enforce a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.
Insure that privileged users have separate accounts for privileged functions and non-privileged functions. Set up and enforce procedures to ensure that do not use their privileged account for non-privileged functions.

Notes:

TCM.0016 V0012978 CAT II TCM.0016

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.5.2.5

Vulnerability Access and use of pervasive device software libraries was not restricted to IAM documented authorized personnel.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment and customer data.

Checks TCM.0016

Ensure that the IAO restricts access and use of pervasive device software libraries to IAM documented authorized personnel

Default Finding Details Access and use of pervasive device software libraries was not restricted to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0016

Insure proper DACLs are in place for directories and files that contain system binaries and they are restricted onl to authorized personnel.

Notes:

TCM.0017 V0012979 CAT II TCM.0017

8500.2 IA Control: DCCS-2 References: Enterprise System Management STIG Section B.5.2.6

Vulnerability The version of JAVA installedto support of the IBM Tivoli Configuration Manager is not at Java 1.3.0 or greater.

Vulnerability Discussion Failure to install a version of JAVA at a level of 1.3.0 or higher is requred for proper support for the web interface for the Tivoli Configuration Manager. Results of installing a lower version is unpredictable.

Checks TCM.0017

Have the SA verify that Java is at least at 1.3.0 version to support the IBM Tivoli Configuration Manager.

Default Finding Details The version of JAVA installed to support of the IBM Tivoli Configuration Manager is not at Java 1.3.0 or greater

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0017

the SA will verify that the version level of JAVA is at a minimumlevel of 1.3.0 to support of the IBM Tivoli Configuration Manager.

Notes:

TCM.0019 V0012980 CAT II TCM.0019

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.5.2.7

Vulnerability The creation, maintenance and deletion of directory query libraries and directory queries are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion

Checks TCM.0019

Have IAO ensure that the creation, maintenance and deletion of directory query libraries and directory queries is limited to the TMR administrator and IAM documented authorized personnel

Default Finding Details The creation, maintenance and deletion of directory query libraries and directory queries are not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0019

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TCM.0022 V0012981 CAT II TCM.0022

8500.2 IA Control: IAIA-2, IAIA-1 References: Enterprise System Management STIG Section B.5.3

Vulnerability The authorization of TCM roles is not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TCM.0022**

Have the IAO ensure that authorization of TCM roles is limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The authorization of TCM roles is not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TCM.0022**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TCM.0023 V0012982 CAT II TCM.0023

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.5.4

Vulnerability The creation, maintenance and deletion of repositories is not limited in accordance with the minimal specifications in the Object Permissions section and the appropriate platform STIGs.

Vulnerability Discussion Use of approved configuration guidance insures the system is initially free of security issues inherent in newly deployed IA and IA enabled products.

Checks **TCM.0023**

Have IAO will ensure the creation, maintenance and deletion of repositories is limited in accordance with the minimal specifications in the Object Permissions section and the appropriate platform STIGs.

Default Finding Details The creation, maintenance and deletion of repositories is not limited in accordance with the minimal specifications in the Object Permissions section and the appropriate platform STIGs.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TCM.0023**

Implement policy and procedures that requires the SAs and NAs use DOD approved or other acceptable configuration security documents as their primary source of security guidance.

Notes:

TCM.0024 V0012984 CAT II TCM.0024

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.5.4

Vulnerability Passwords used by the RIM objects and the RDBMS do not comply with the password specifications listed in the Database STIG.

Vulnerability Discussion Failure to properly identify individuals along with Inadequate Individual Identification and Authentication before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TCM.0024**

The IAO will ensure passwords used by the RIM objects and the RDBMS comply with the password guidelines specified Database STIG.

Default Finding Details Passwords used by the RIM objects and the RDBMS do not comply with the password specifications listed in the Database STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0024**

Ensure passwords used by the RIM objects and the RDBMS comply with the password guidelines specified Database STIG.

Notes:

TCM.0025 V0012985 CAT II TCM.0025

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.5.4

Vulnerability The creation, maintenance and deletion of RIM objects are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TCM.0025**

Have the IAO ensure the creation, maintenance and deletion of RIM objects are limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation, maintenance and deletion of RIM objects are not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TCM.0025**

Verify that the ability to creat, maintain or delete RIM objects are limited to the TMR administrator and IAM documented authorized personnel

Notes:

TCM.0027 V0012986 CAT II TCM.0027

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.5.5

Vulnerability The creation, maintenance and deletion of reference models are not restricted to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TCM.0027

Have the IAO ensure the creation, maintenance and deletion of reference models are restricted to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation, maintenance and deletion of reference models are not restricted to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0027

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TCM.0030 V0012987 CAT II TCM.0030

8500.2 IA Control: ECWN-1 References: Enterprise System Management STIG Section B.5.8

Vulnerability Pervasive device access is not properly restricted

Vulnerability Discussion Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are easily exploited by outsiders and easily misused by users. Results can be loss or compromise of sensitive data and/or compromise of the system.

Checks TCM.0030

Collect finding information from the wireless discovery and wireless device reviewer(s) to identify active wireless services. Verify that all implemented wireless services are documented in the SSAA and approved by the DAA.
Verify that local site documentation includes instructions to users on operation of approved and unapproved wireless services.
Verify that local documentation requires that imbedded wireless services be disabled unless specifically authorized by the DAA.
Verify that Wireless computing capabilities are not independently configurable by the users.

Default Finding Details Pervasive device access is not properly restricted

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0030

Implement wireless computing and networking capabilities workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices in accordance with DoD wireless policy.
Document all wireless services in the SSAA. Include instructions to users on operation of approved and unapproved wireless services in local site documentation.
Implement and enforce procedures to require that imbedded wireless services be disabled unless specifically authorized by the DAA. Implement and enforce procedures to prevent wireless computing and networking capabilities from being independently configured
by end users.

Notes:

TCM.0031 V0012988 CAT II TCM.0031

8500.2 IA Control: ECWN-1 References: Enterprise System Management STIG Section B.5.8

Vulnerability Pervasive device access is limited to IAM documented authorized personnel.

Vulnerability Discussion Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are easily exploited by outsiders and easily misused by users. Results can be loss or compromise of sensitive data and/or compromise of the system.

Checks TCM.0030

Collect finding information from the wireless discovery and wireless device reviewer(s) to identify active wireless services. Verify that all implemented wireless services are documented in the SSAA and approved by the DAA.
Verify that local site documentation includes instructions to users on operation of approved and unapproved wireless services.
Verify that local documentation requires that imbedded wireless services be disabled unless specifically authorized by the DAA.
Verify that Wireless computing capabilities are not independently configurable by the users.

Default Finding Details Pervasive device access is limited to IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0030

Implement wireless computing and networking capabilities workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices in accordance with DoD wireless policy.
Document all wireless services in the SSAA. Include instructions to users on operation of approved and unapproved wireless services in local site documentation.
Implement and enforce procedures to require that imbedded wireless services be disabled unless specifically authorized by the DAA. Implement and enforce procedures to prevent wireless computing and networking capabilities from being independently configured
by end users.

Notes:

TCM.0033 V0012989 CAT II TCM.0033

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.5.9

Vulnerability IBM Tivoli Configuration Manager directories not protected from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of the ESM Tivoli STIG.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks TCM.0033

Ensure that the SA restricts the IBM Tivoli Configuration Manager directories from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of the ESM TIVOLI STIG.

Default Finding Details IBM Tivoli Configuration Manager directories not protected from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of the ESM Tivoli STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0033

Configure the system to establish control mechanisms to ensure that TIVOLI data is accessed and changed only by authorized personnel.

Notes:

TCM.0035 V0012990 CAT II TCM.0035

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.5.9

Vulnerability The IBM Tivoli Configuration Manager directories on the secondary event servers are not restricted from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of the ESM Tivoli STIG.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks TCM.0035

Ensure that The SA restricts the IBM Tivoli Configuration Manager directories on the secondary event servers from unauthorized access and updates, verify access control mechanisms have been established and are working to ensure that data is accessed and changed only by authorized personnel.

Default Finding Details The IBM Tivoli Configuration Manager directories on the secondary event servers are not restricted from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of the ESM Tivoli STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0035

Configure the system to establish control mechanisms to ensure that data is accessed and changed only by authorized personnel.

Notes:

TCM.0036 V0012991 CAT II TCM.0036

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.5.9

Vulnerability Access to the subdirectories of the BINDIR directory, its subdirectories, and all files in those subdirectories on Windows Gateway systems is not restricted in accordance with in the Object Permissions section and the Windows STIG.

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks TCM.0036

The SA will restrict access to the subdirectories of the BINDIR directory, its subdirectories, and all files in those subdirectories on Windows Gateway systems

Default Finding Details Access to the subdirectories of the BINDIR directory, its subdirectories, and all files in those subdirectories on Windows Gateway systems is not restricted in accordance with in the Object Permissions section and the Windows STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0036

Establish access control mechanisms to ensure that data is accessed and changed only by authorized personnel.
Ensure transaction logs record access and changes to the data. Establish and enforce procedures to ensure the transaction logs are reviewed periodically (monyhly at a minimum) and immediately upon system security events.
Implement a process to notify users of time and date of the last change in data content.

Notes:

TCM.0037 V0012992 CAT II TCM.0037

8500.2 IA Control: ECCD-1, ECCD-2 References: Enterprise System Management STIG Section B.5.9

Vulnerability Access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems is not restricted in accordance with in the Object Permissions section in the ESM Tivoli STIG..

Vulnerability Discussion Without access control the data is not secure. It can be compromised, misused or changed by unauthorized access at any time.

Checks TCM.0037

The SA will restrict access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems in accordance and verify access control mechanisms have been established and are working to ensure that data is accessed
and changed only by authorized personnel.

Default Finding Details Access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems is not restricted in accordance with in the Object Permissions section in the ESM Tivoli STIG..

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TCM.0037

Configure the system to establish control mechanisms to ensure that data is accessed and changed only by authorized personnel.

Notes:

TEC.0011 V0012905 CAT II TEC.0011

8500.2 IA Control: COTR-1 References: Enterprise System Management STIG Section B..2.1

Vulnerability Inadequate Recovery Procedures

Vulnerability Discussion Improper system recovery can result in loss or compromise of sensitive information and/or compromise of the system by unauthorized individuals who seize the opportunity to exploit known vulnerabilities. Tivoli requires a trusted recovery of the TMR, policy regions, managed nodes and gateways in the event of a technical failure.

Checks TEC.0011

The TMR administrator, TEC administrator and Tivoli administrators will maintain documentation as part of the disaster recovery plan describing the procedures necessary to perform a trusted recovery of the TEC to include the event server, database, adapter files, software and configuration files.

Default Finding Details The following issues were noted: Recovery procedures and technical system features do not exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are not documented. Circumstances that can inhibit trusted recover are documented but appropriate mitigating procedures are not in place. There is no list of personnel authorized to perform the recover function.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0012

Insure that the DRP or SOP has recovery procedures that indicate the steps needed for secure recovery. Verification process can include original COTS or GOTS installation media or a hash of the installation program. These procedures should include any special considerations for trusted recovery such as network attachment or placement. The procedure should also include the list of authorized personnel that perform the function.

Notes:

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks TME.0001

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TME.0001

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0007 V0012900 CAT II TMF.0007

8500.2 IA Control: DCCS-1, DCCS-2 References: Enterprise System Management STIG Section B.2.1

Vulnerability Systems hosting TIVOLI Sostware will be configured as specified in the ESM STIG.

Vulnerability Discussion Due to the capabilities of TIVOLI software to alter information on the systems it controls. It is important to properly secure the TIVOLI software.

Checks TMF.0007

Verify with the IAM that the Tivoli software was installed following the configuration specified in the ESM STIG and the STIG of the system it was installed on. If installed on WINDOWS or UNIX systems, verify that physical security of the platforms, network connectivity, file access controls, change management and backups and recovery be addressed so as to ensure the confidentiality, availability and integrity of the Tivoli Enterprise and the resources that exist in it.

Default Finding Details The following TIVOLI Managegment software was not configued as specified in the ESM STIG and the STIG of the system it was installed on.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMF.0007

When installing TIVOLI software validate that it is configred as specified in the ESM STIG and the STIG of the system it was installed on.

Notes:

TMF.0010 V0012903 CAT III TMF.0010

8500.2 IA Control: CODP-2 References: Enterprise System Management STIG Section b.2.1

Vulnerability Inadequate Disaster Recovery Plan

Vulnerability Discussion Disaster Recovery Plan does not allow for the resumption of mission or business critical functions within 24 hours.

Checks **TMF.0010**

The IAM will ensure that a written plan exists that addresses the partial resumption of mission or business essential functions with 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Default Finding Details Well thought out recovery plans are essential for system recovery and/or business restoral in the event of catastrophic failure or disaster.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0010**

The Tivoli administrator must Develop a Disaster Recovery Plan for the Information System or Facility that Insures the plan:
provides for partial resumption of function within 24 hours
contains business recovery plans
contains system contingency plans
contains facility disaster recovery plans
is officially accepted by the IS or facility owner

Notes:

TMF.0022 V0012914 CAT II TMF.0022

8500.2 IA Control: ECTB-1 References: Enterprise System Management STIG Section B.2.2.3

Vulnerability The httpserv.log and the httptran.log files are not included as part of the regularly scheduled site backups.

Vulnerability Discussion Audit records provide the means for the IAO or other designated person to investigate any suspicious activity and to hold users accountable for their actions. If the records are not properly stored and protected, the IAO or other designated personnel will be able to unable to detect and investigate suspicious activity.

Checks **TMF.0022**

Verify with the IAO that the httpserv.log and the httptran.log files are backed up weekly and stored on different media.

Default Finding Details The httpserv.log and the httptran.log files are not are backed up weekly onto a different system or media than the system being audited.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0022**

Verify that the the httpserv.log and the httptran.log files are included on the list of weekly backup files.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

TMF.0064 V0012955 CAT II TMF.0064

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.2.11.1

Vulnerability All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMF.0064**

The IAO will ensure all installations and updates to the Tivoli AEF are restricted to the SA, the TMR administrator and IAM documented authorized personnel.

Default Finding Details All installations and updates to the Tivoli AEF are not restricted to the SA, the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0064**

Implement the IA Control IAIA-1. Specifically:
Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

12. CHECKLIST INSTRUCTIONS – Tivoli Monitoring for Business Integration Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the Tivoli Monitoring for Business Integration Checks that must be reviewed if reviewing Tivoli Monitoring for Business Integration. Sections 1- 4 of this checklist are required to be completed prior to reviewing this section.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., guidance for marking N/A is included in the instructions). If vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed”. Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

TME.0001 V0012690 CAT II TME.0001

8500.2 IA Control: DCCS-1, DCCS-2, DCPR-1 References: Enterprise System Management STIG Section B.1

Vulnerability A current configuration document for each system does not exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This vulnerability will also cover TMF.0001, TEC.0001, TIM.0001, TCM.0001, and TMQ.0001.

Vulnerability Discussion To properly review an ESM system for possible vulnerabilities, you need a complete understanding of the configuration and all the components that make up the enterprise. ESM configuration diagrams and inventories provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

Checks **TME.0001**

Have the IAO/IAM verify with the ESM administrator that configuration documents exist in the SSAA that describes all the components that make up the Tivoli Management Environment. This includes TMF,TEC,TIM,TCM and TMQ components.

Default Finding Details The following TIVOLI environemets have incomplete configuration and inventory information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TME.0001**

The IAO will make sure that the SSAA contains complete configuration diagrams and inventory describing the ESM System and all of its components.

Notes:

TMF.0003 V0012779 CAT II TMF.0003

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.2.1

Vulnerability TMF software not being protected from unauthorized use.

Vulnerability Discussion The TMF software is very powerful and must be protected from unathorized use, to avoid attacks on other systems or introduction of unathorized code.

Checks **TMF.0003**

Have the IAO verify that all software modules and libraries are restricted to ESM authorized users

Default Finding Details The following software libraries were not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0003**

Have the IAO validate that all libraries containing TMF modules are properly protected and open only to authorized users.

Notes:

TMF.0017 V0012909 CAT II TMF.0017

8500.2 IA Control: DCSP-1, PRNK-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Tivoli desktops are not located in an area, which is restricted from unauthorized access and protected by the local firewall.

Vulnerability Discussion The Tivoli Desktop is the standard graphical user interface (GUI) provided by Tivoli that enables administrators to communicate with the TMF and the other Tivoli products in the Tivoli Enterprise.Due to the capabilities to control the enterprise, these systems must be resticted to authorized users and protected .

Checks **TMF.0017**

Verify with the IAM and the Network Security Officer that Tivoli desktops are restricted from unauthorized access and are protected by a firewall.

Default Finding Details The TIVOLI desktop was not restricted to authorized user and was not properly protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0017**

Make sure that TIVOLI Desktops are restricted to only authorized personnel and that they are located behind a firewall.

Notes:

TMF.0018 V0012910 CAT II TMF.0018

8500.2 IA Control: DCSP-1 References: Enterprise System Management STIG Section B.2.2.1

Vulnerability Access to Tivoli desktops is not restricted to policy regions.

Vulnerability Discussion A policy region is a logical collection of resources that are controlled by one or more policies. The set of managed resources that may exist in a policy region depends on the applications and the products installed in the TMR. Resource access is controlled when resources are organized in policy regions and authorization roles are assigned at the resource level. In this way Tivoli Desktops are limited to only those resources contained within the policy.

Checks **TMF.0018**

Have the TIVOLI Administrator show that the TIVOLI desktop is resticted by policy region.

Default Finding Details The following desktops were not limited to thier policy region.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0018**

The TIVOLI Administrator will establish poicy regions as part of the TIVOLI installation to control resources.

Notes:

TMF.0058 V0012949 CAT III TMF.0058

8500.2 IA Control: DCBP-1 References: Enterprise System Management STIG Section B.2.8

Vulnerability Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

Vulnerability Discussion Use of security best practices makes security implementation and checking easier and results in fewer security problems. Security designs should follow approporiate security guidance and employ DOD Defense in depth techniques.

Checks **TMF.0058**

The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.

Default Finding Details Unauthorized directories/files, including expired releases of Tivoli software, exist in the currently distributed Tivoli directories.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMF.0058**

Have the Tivoli administrator verify that the levels of the software being installed are suported and unexpired.

Notes:

TMQ.0007 V0013028 CAT II TMQ.0007

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.6.1

Vulnerability The creation, distribution and implementation of Tivoli Monitoring for Business Integration endpoint monitors and resource models is not limited to TMR administrators and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks **TMQ.0007**

Verify that the IAO ensures the creation, distribution and implementation of Tivoli Monitoring for Business Integration endpoint monitors and resource models is limited to TMR administrators and IAM documented authorized personnel.

Default Finding Details The creation, distribution and implementation of Tivoli Monitoring for Business Integration endpoint monitors and resource models is not limited to TMR administrators and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes **TMQ.0007**

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMQ.0009 V0013029 CAT II TMQ.0009

8500.2 IA Control: IAIA-1, IAIA-2 References: Enterprise System Management STIG Section B.6.2.1

Vulnerability The creation, maintenance and distribution of all WebSphereMQ resources and profiles are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Failure to properly identify individuals before allowing access to DOD Information Systems could result in theft or loss of sensitive or classified information.

Checks TMQ.0009

Verify that the IAO ensures the creation, maintenance and distribution of all WebSphereMQ resources and profiles are limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details The creation, maintenance and distribution of all WebSphereMQ resources and profiles are not limited to the TMR administrator and IAM documented authorized personnel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMQ.0009

Require that access to the system be gained through a two-factor authentication system (e.g., a unique token or user logon ID and password)

Notes:

TMQ.0010 V0013030 CAT II TMQ.0010

8500.2 IA Control: DCSL-1 References: Enterprise System Management STIG Section B.6.2.1

Vulnerability The creation, maintenance and distribution of all Tivoli Monitoring for Business Integration tasks and task libraries are not limited to the TMR administrator and IAM documented authorized personnel.

Vulnerability Discussion Liibraries contain program modules which possess a significant level of security bypass capability. Unauthorized access could result in the compromise of the operating system environment, and customer data.

Checks TMQ.0010

The IAO will ensure the creation, maintenance and distribution of all Tivoli Monitoring for Business Integration tasks and task libraries are limited to the TMR administrator and IAM documented authorized personnel.

Default Finding Details he creation, maintenance and distribution of all Tivoli Monitoring for Business Integration tasks and task libraries are not limited to the TMR administrator and IAM documented authorized personnel.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMQ.0010

Insure proper DACLs are in place for directories and files that contain system binaries.

Notes:

TMQ.0011 V0013031 CAT II TMQ.0011

8500.2 IA Control: COTR-1

References: Enterprise System Management STIG Section B.6.2.2

Vulnerability All Tivoli Monitoring for Business Integration remote administration consoles are not located on a platform is secured in accordance with the appropriate platform STIGs.

Vulnerability Discussion A comprehensive annual IA review that evaluates existing policies and processes is necessary to ensure consistency and to ensure that procedures fully support the goal of uninterrupted operations.

Checks TMQ.0011

Verify that the IAO will ensure all Tivoli Monitoring for Business Integration remote administration consoles are located on a platform is secured in accordance with the appropriate platform STIGs.

Default Finding Details All Tivoli Monitoring for Business Integration remote administration consoles are not located on a platform is secured in accordance with the appropriate platform STIGs.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes TMQ.0011

Arrange for, or perform a comprehensive IA review every 12 months.

Notes: