

When this document is printed, the document needs to be stamped top and bottom with the appropriate classification.

VL05 - Checklist 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

Checklist: Generic Database Installation

Vulnerability Key: V0005658

STIG ID: DG0001

Release Number: 14

Status: Active

Short Name: DBMS version support

Long Name: Vendor supported software is evaluated and patched against newly found vulnerabilities.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0001-Generic

Severity: Category I

Severity Override: If the DBMS host is not connected to a production network and is on an isolated development or test network segment and an upgrade plan is in place, the severity of this finding may be downgraded to a CAT 2.

Vulnerability

Unsupported software versions are not patched by vendors to address newly discovered security

Discussion: versions. An unpatched version is vulnerable to attack.

Default Finding Details: Software not supported by the vendor is not evaluated or patched against newly found vulnerabilities.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation VIVM-1

Checks: DB-DG0001-Generic (Manual)

Follow the vendor instruction for determining the product version number.

View the vendor-provided list of supported versions. To be considered supported, the vendor must report that the version is supported by security patches to reported vulnerabilities.

If the security patch support for the installed version cannot be determined or the version is not shown as supported, this is a Finding.

If the installation is not connected to a production network and is on an isolated development or test network segment and an upgrade plan is in place, the severity of this finding may be downgraded to a CAT 2.

Fixes: DB-DG0001-Generic (Manual)

Develop, document and implement policy and procedures to upgrade the DBMS to a vendor-supported version.

Vulnerability Key: V0004758

STIG ID: DG0002

Release Number: 14

Status: Active

Short Name: DBMS version upgrade plan

Long Name: An upgrade/migration plan should be developed to address an unsupported DBMS software version.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0002-Generic

Severity: Category II

Severity**Override****Guidance:****Vulnerability****Discussion:**

Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack. Developing and implementing an upgrade plan prior to a lapse in support helps to protect against published vulnerabilities.

Default**Finding****Details:**

An upgrade/migration plan has not been developed to address an unsupported DBMS software version.

Documentable: No

Documentable**Explanation:**

Responsibility: Information Assurance Officer

References:

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation VIVM-1

Checks:

DB-DG0002-Generic (Interview)

If the check for unsupported version (DG0001) returns an unsupported version or the installed version is within 6 mos. of a desupport notice, ask if migration plans are in progress to upgrade to a supported version.

If plans are not in progress, this is a Finding.

Review evidence that extended support has been purchased for product versions that are no longer in mainstream support.

If product version is in extended support and an extended support contract has not been purchased, this is a Finding.

If Extended Support will expire within 6 months, ask the IAO to provide evidence that an upgrade to a supported version or an extension to the support is planned and in progress.

If it is not evident, this is a Finding.

Fixes:

DB-DG0002-Generic (Manual)

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 scheduled for completion prior to expiration of the current product or product support contract.

Vulnerability Key: V0005659

STIG ID: DG0003

Release Number: 10

Status: Active

Short Name: DBMS security patch level

Long Name: The latest security patches should be installed.

Comments:

- ☐ Open
- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0003-Generic

Severity: Category II

Severity Override Guidance: If any security patches are not installed that the vendor has deemed critical, the severity of this check should be upgraded to CAT 1.

Vulnerability Discussion: Maintaining the currency of the software version protects the database from known vulnerabilities.

Default Finding Details: The latest security patches have not been installed.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation VIVM-1

Checks: DB-DG0003-Generic (Manual)
Search the DBMS vendor web site for available security patches.

If all security patches available for the installed version have not been applied, this is a Finding.

Note: If any security patches are not installed that the vendor has deemed critical, the severity of this check should be upgraded to CAT 1.

Fixes: DB-DG0003-Generic (Manual)
Apply all security updates to the database software. Follow vendor-provided patch installation instructions.

Vulnerability Key: V0006756

STIG ID: DG0005

Release Number: 9

Status: Active

Short Name: DBMS administration OS accounts

Long Name: Only necessary privileges to the host system should be granted to DBA OS accounts.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0005-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Database administration accounts are frequently granted more permissions to the local host system than are necessary. This allows inadvertent or malicious changes to the host operating system.

Default Finding Details: Unnecessary privileges to the host system have been granted to DBA OS accounts.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0005-Generic (Manual)
Review host system privileges assigned to the DBA accounts. If any are granted host system administrator privileges or other system privileges not required for DBMS administration, this is a Finding.

Fixes: DB-DG0005-Generic (Manual)
Revoke any host system privileges from DBA accounts not required for DBMS administration. Revoke any OS group memberships that assign excess privileges to DBA accounts. Remove any directly applied permissions or user rights from the DBA account.

Vulnerability Key: V0006767

STIG ID: DG0007

Release Number: 6

Status: Active

Short Name: DBMS security compliance

Long Name: The database should be secured in accordance with DoD, vendor and/or commercially accepted practices where applicable.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0007-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: DBMS systems that do not follow DoD security guidance are vulnerable to related published vulnerabilities. A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities.

Default Finding Details: The database has not been secured in accordance with DoD guidance where applicable.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCCS-2

Checks: DB-DG0007-2-Generic (Manual)
Review security and administration documentation maintained for the DBMS system for indications that DoD security guidance has been applied to the DBMS system.

If the DBMS system has not been secured using available DoD security guidance, this is a Finding.

Fixes: DB-DG0007-2-Generic (Manual)
Apply available DoD security guidance to the DBMS system.

If DoD security guidance is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a departmental reference guide.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0007-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: DBMS systems that do not follow DoD, vendor and/or public best security practices are vulnerable to related published vulnerabilities. A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities.

Default Finding Details: The database has not been secured in accordance with DoD, vendor and/or commercially accepted practices where applicable.

Documentable: No

Documentable

Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCCS-1

Checks: DB-DG0007-1-Generic (Manual)

Review security and administration documentation maintained for the DBMS system for indications that security guidance has been applied to the DBMS system.

If DoD security guidance is not available, the following are acceptable in descending order as available:

- (1) Commercially accepted practices (e.g., SANS);
- (2) Independent testing results (e.g., ICISA); or
- (3) Vendor literature

If the DBMS system has not been secured using available security guidance as listed above, this is a Finding.

Fixes: DB-DG0007-1-Generic (Manual)

Apply available security guidance to the DBMS system.

If DoD security guidance is not available, the following are acceptable in descending order as available:

- (1) Commercially accepted practices (e.g., SANS);
- (2) Independent testing results (e.g., ICISA); or
- (3) Vendor literature

Vulnerability Key: V0015608

STIG ID: DG0009

Release Number: 4

Status: Active
Short Name: DBMS software library permissions
Long Name: Access to DBMS software files and directories should not be granted to unauthorized users.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0009-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The DBMS software libraries contain the executables used by the DBMS to operate. Unauthorized access to the libraries can result in malicious alteration or planting of operational executables. This may in turn jeopardize data stored in the DBMS and/or operation of the host system.

Default Finding Details: Access to DBMS software files and directories are granted to unauthorized users.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSL-1

Checks: DB-DG0009-Generic (Manual)
 Review permissions that control access to the DBMS software libraries.
 The software library location may be determined from vendor documentation or service/process executable paths.

DBA accounts, the DBMS process account, the DBMS software installation/maintenance account, SA accounts if access by them is required for some operational level of support such as backups, and the host system itself require access.

Compare the access control employed with that documented in the System Security Plan.

If access controls do not match the documented requirement, this is a Finding.

If access controls appear excessive without justification, this is a Finding.

Fixes: DB-DG0009-Generic (Manual)
 Restrict access to the DBMS software libraries to the fewest accounts that clearly require access based on job function.

Document authorized access control and justify any access grants that do not fall under DBA, DBMS process, ownership, or SA accounts.

Vulnerability Key: V0002420

STIG ID: DG0010

Release Number: 15

Status: Active

Short Name: DBMS software monitoring

Long Name: Database executable and configuration files should be monitored for unauthorized modifications.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0010-Generic

Severity: Category III

Severity

Override

Guidance:

Vulnerability Discussion: Changes to files in the DBMS software directory including executable, configuration, script, or batch files can indicate malicious compromise of the software files. Changes to non-executable files, such as log files and data files, do not usually reflect unauthorized changes, but are modified by the DBMS as part of normal operation. These modifications can be ignored.

Default Finding Details: Database executable and configuration files are not being monitored for unauthorized modifications.

Documentable: No

Documentable

Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSL-1

Checks: DB-DG0010-Generic (Interview)

Review with the DBA any software modification detection procedures in place and request documents of these procedures to review.

If procedures do not exist that include review of the database software directories and database application directories, this is a Finding.

Fixes: DB-DG0010-Generic (Manual)

Develop, document and implement procedures to monitor any changes made to the database software.

Identify all database files and directories to be included in the host system or database backups and provide these to the person responsible for backups.

For Windows systems, you can use the `dir /s > filename.txt` run weekly to store and compare file modification/creation dates and file sizes using the DOS `fc` command.

For UNIX systems, you can use the `ls -as >filename.txt` command to store and compare (diff command) file statistics for comparison.

These are not as comprehensive as some tools available, but may be enhanced by including checks for checksums or file hashes.

Vulnerability Key: V0003726

STIG ID: DG0011

Release Number: 15

Status: Active

Short Name: DBMS Configuration Management

Long Name: Configuration management procedures should be defined and implemented for database software modifications.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0011-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Uncontrolled, untested, or unmanaged changes result in an unreliable security posture. All changes to software libraries related to the database and its use need to be reviewed, considered, and the responsibility for CM assigned. CM responsibilities may appear to cross boundaries. It is important, however, for the boundaries of CM responsibility to be clearly defined and assigned to ensure no libraries or configurations are left unaddressed. Related database application libraries may include third-party DBMS management tools, DBMS stored procedures, or other end-user applications.

Default Finding Details: Configuration management procedures are not defined and implemented for database software modifications.

Documentable: No

Documentable**Explanation:****Responsibility:** Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPR-1

Checks: DB-DG0011-Generic (Interview)

Interview the IAO and review documentation to determine if a configuration management (CM) process is implemented for the DBMS system that includes requirements for:

(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;

(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(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.

If documented evidence for procedures or processes outlined above are not present or are incomplete, this is a Finding.

Fixes: DB-DG0011-Generic (Manual)

Develop, document and implement configuration management procedures or processes.

Ensure the 4 major requirements listed in the check are documented at a minimum.

Assign responsibilities for oversight and approval for any and all changes made to DBMS software and configuration.

Vulnerability Key: V0004754**STIG ID:** DG0012**Release Number:** 11**Status:** Active**Short Name:** DBMS software storage location

Long Name: Database software directories including DBMS configuration files are stored in dedicated directories separate from the host OS and other applications.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)**Policy:** All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0012-Generic**Severity:** Category II**Severity****Override****Guidance:**

Vulnerability Discussion: Multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to host system directories can most likely lead to a compromise of all applications hosted by the same system. Database software not installed using dedicated directories both threatens and is threatened by other hosted applications. Access controls defined for one application may by default provide access to the other application's database objects or directories. Any method that provides any level of separation of security context assists in the protection between applications.

Default Finding Details:

Database software directories including DBMS configuration files are not stored in dedicated directories separate from the host OS and other applications.

Documentable: No**Documentable****Explanation:****Responsibility:** Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPA-1

Checks: DB-DG0012-Generic (Manual)

Review the DBMS software library directory and note other root directories located on the same disk directory or any subdirectories within the DBMS software library directory.

If any other non-DBMS software directories exist on the disk directory, examine or investigate their use.

If any of the directories are used by other applications including third-party applications that use the DBMS, this is a Finding.

Only applications that are required for the functioning and administration, not use, of the DBMS should be located on the same disk directory as the DBMS software libraries.


Fixes: DB-DG0012-Generic (Manual)

Install all applications on directories separate from the DBMS software library directory.

Re-locate any directories or re-install other application software that currently shares the DBMS software library directory to separate directories.

Recommend dedicating a separate partition for the DBMS software libraries where supported by the DBMS.

Vulnerability Key: V0015126**STIG ID:** DG0013**Release Number:** 9**Status:** Active**Short Name:** DBMS backup procedures**Long Name:** Database backup procedures should be defined, documented and implemented.

 Open	Comments:
------------------------------------------------------------------------------------------	-----------

- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0013-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Database backups provide the required means to restore databases after compromise or loss.

Backups help reduce the vulnerability to unauthorized access or hardware loss.

Default Finding Details: Database backup procedures are not defined, documented or implemented.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation CODB-1

Checks: DB-DG0013-1-Generic (Interview)

Review the database backup procedures and implementation evidence.

Evidence of implementation includes records of backup events and physical review of backup media.

Evidence should match the backup plan as recorded in the System Security Plan.

If backup procedures do not exist or not implemented in accordance with the procedures, this is a Finding.

If backups are not performed weekly or more often, this is a Finding.

Fixes: DB-DG0013-1-Generic (Manual)

Develop, document and implement database backup procedures.

Include weekly backup procedures and offline backup data storage.

- ☐ Open
- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Comments:

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0013-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Database backups provide the required means to restore databases after compromise or loss. Backups help reduce the vulnerability to unauthorized access or hardware loss.

Default Finding Details: Database backup procedures are not defined, documented or implemented.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation CODB-2

Checks: DB-DG0013-2-Generic (Interview)

Review the database backup procedures and implementation evidence.

Evidence of implementation includes records of backup events and physical review of backup media.

Evidence should match the backup plan as recorded in the System Security Plan.

If backup procedures do not exist or not implemented in accordance with the procedures, this is a Finding.

If backups are not performed daily or more often, this is a Finding.

If backup data is not secured and stored offline at an alternate site, this is a Finding.

Fixes: DB-DG0013-2-Generic (Manual)

Develop, document and implement database backup procedures.

Include daily backup procedures and offline backup data storage at an alternate site.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0013-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Database backups provide the required means to restore databases after compromise or loss. Backups help reduce the vulnerability to unauthorized access or hardware loss.

Default Finding Details: Database backup procedures are not defined, documented or implemented.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation CODB-3

Checks: DB-DG0013-3-Generic (Manual)
Review the database backup procedures and implementation evidence.

Evidence of implementation includes records of backup events and physical review of backup media.

Evidence should match the backup plan as recorded in the System Security Plan.

If backup procedures do not exist or not implemented in accordance with the procedures, this is a Finding.

If backups do not include a redundant secondary system maintained at a separate physical site that can be activated without interruption or loss of data if the primary system fails, this is a Finding.

Fixes: DB-DG0013-3-Generic (Manual)
Develop, document and implement database backup procedures.

Include a secondary server installed at a separate location (IAW COOP guidelines) that can be brought online to prevent any disruption to availability or loss of data.

Vulnerability Key: V0015609

STIG ID: DG0014

Release Number: 5

Status: Active

Short Name: DBMS demonstration and sample databases

Long Name: Default demonstration and sample database objects and applications should be removed.

<input type="checkbox"/> Open	Comments:
-------------------------------	-----------

☐ Not a Finding

☐ Not Applicable

☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0014-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Demonstration and sample database objects and applications present publicly known attack points for malicious users. These demonstration and sample objects are meant to provide simple examples of coding specific functions and are not developed to prevent vulnerabilities from being introduced to the DBMS and host system.

Default Finding Details: Default demonstration and sample database objects and applications have not been removed.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0014-Generic (Manual)

Review vendor documentation and vendor web sites for vendor-provided demonstration or sample database applications, objects and files.

Review the DBMS to determine if any of the demonstration and sample objects, applications or files are installed in the database or are included with the DBMS application.

If any are present in the database or are included with the DBMS application, this is a Finding.

Fixes: DB-DG0014-Generic (Manual)

Remove any known demonstration and sample applications, objects and files from the DBMS.

Vulnerability Key: V0003728

STIG ID: DG0016

Release Number: 11

Status: Active

Short Name: DBMS unused components

Long Name: Unused database components, database application software and database objects should be

removed from the DBMS system.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0016-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Unused, unnecessary DBMS components increase the attack vector for the DBMS by introducing additional targets for attack. By minimizing the services and applications installed on the system, the number of potential vulnerabilities is reduced.

Default Finding Details: Unused database components, database application software or database objects have not been removed from the DBMS system.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0016-Generic (Interview)

Review the list of components and features installed with the database.

Use the DBMS product installation tool if supported and review the product installation documentation.

If no unused features or components are installed, this is Not a Finding.

If unused components or features are installed, review the System Security Plan to verify that they are documented and authorized.

If any are not documented and authorized, this is a Finding.

Fixes: DB-DG0016-Generic (Manual)

If any components or features are required for operation of applications that will be accessing the DBMS, include them in the application design specification and list in the System Security Plan.

If any unused components or features are installed and can be uninstalled, uninstall them and remove any database objects and applications that are installed to support them.

Where uninstallation is not possible, document in the System Security Plan as such.

Vulnerability Key: V0003803

STIG ID: DG0017

Release Number: 12

Status: Active

Short Name: DBMS shared production/development use

Long Name: A production DBMS installation should not coexist on the same DBMS host with other, non-production DBMS installations.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0017-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Production, development and other non-production DBMS installations have different access and security requirements. Shared production/non-production DBMS installations secured at a production-level can impede development efforts whereas production/non-production DBMS installations secured at a development-level can lead to exploitation of production-level installations. Production DBMS installations should be kept separate from development, QA, TEST and other non-production DBMS systems.

Default Finding Details: A production DBMS installation coexists on the same DBMS host with other, non-production DBMS installations.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECSD-1, ECSD-2

Checks: DB-DG0017-Generic (Interview)

Review the System Security Plan and interview the DBA and IAO to determine if the DBMS host contains production and non-production DBMS installations.

If the DBMS host contains both production and non-production DBMS installations or the production DBMS installation is being used for non-production efforts, determine if this allowance

is documented in the System Security Plan and authorized by the IAO.

If not documented and authorized, this is a Finding.

NOTE: Though shared production/non-production DBMS installations was allowed under previous database STIG guidance, doing so may place it in violation of OS, Application, Network or Enclave STIG guidance. Ensure that any shared production/non-production DBMS installations meets STIG guidance requirements at all levels or mitigate any conflicts in STIG guidance with your DAA.

Fixes: DB-DG0017-Generic (Manual)
Recommend establishing a dedicated DBMS host for production DBMS installations (See Checks DG0109 and DG0110).

A dedicated host system in this case refers to an instance of the operating system at a minimum.

The operating system may reside on a virtual host machine where supported by the DBMS vendor.

Vulnerability Key: V0003805

STIG ID: DG0019

Release Number: 10

Status: Active

Short Name: DBMS software ownership

Long Name: Application software should be owned by a Software Application account.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0019-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: File and directory ownership imparts full privileges to the owner. These privileges should be restricted to a single, dedicated account to preserve proper chains of ownership and privilege assignment management

Default Finding Details: Application software is not owned by a Software Application account.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSL-1

Checks: DB-DG0019-Generic (Manual)

Review the ownership of all DBMS and dependent application software and configuration files.

If the owner is other than the software installation account or the designated owner account for the file, this is a Finding.

Some configuration and log files may be owned by a service or process account.

Ownership of these files should be recorded and verified accordingly.

Fixes: DB-DG0019-Generic (Manual)

Assign DBMS file and directory ownership to the software installation and maintenance account.

Use the software owner account to install and maintain the DBMS software libraries and configuration files.

Vulnerability Key: V0015129

STIG ID: DG0020

Release Number: 9

Status: Active

Short Name: DBMS backup and recovery testing

Long Name: Backup and recovery procedures should be developed, documented, implemented and periodically tested.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0020-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Problems with backup procedures or backup media may not be discovered until after a recovery is needed. Testing and verification of procedures provides the opportunity to discover oversights, conflicts, or other issues in the backup procedures or use of media designed to be used.

Default

Finding Details: Backup and recovery procedures have not been developed, documented, implemented or periodically tested.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
CODP-1, CODP-2, CODP-3

Checks: DB-DG0020-Generic (Interview)

Review the testing and verification procedures documented in the System Security Plan.

Review evidence of implementation of testing and verification procedures by reviewing logs from backup and recovery implementation. Logs may be in electronic or hardcopy and may include email or other notification.

If testing and verification of backup and recovery procedures are not documented in the System Security Plan, this is a Finding.

If evidence of testing and verification of backup and recovery procedures does not exist, this is a Finding.

Fixes: DB-DG0020-Generic (Manual)

Develop, document and implement testing and verification procedures for database backup and recovery.

Include requirements for documenting database backup and recovery testing and verification activities in the procedures.

Vulnerability Key: V0003806

STIG ID: DG0021

Release Number: 11

Status: Active

Short Name: DBMS software and configuration baseline

Long Name: A baseline of database application software should be documented and maintained.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0021-Generic

Severity: Category II

**Severity
Override
Guidance:**

Vulnerability Discussion: Without maintenance of a baseline of current DBMS application software, monitoring for changes cannot be complete and unauthorized changes to the software can go undetected. Changes to the DBMS executables could be the result of intentional or unintentional actions.

Default Finding Details: A baseline of database application software is not documented or maintained.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSW-1

Checks: DB-DG0021-Generic (Interview)
Have the DBA and/or IAO provide the DBMS software baseline procedures, implementation evidence, and a list of files and directories included in the baseline procedure for completeness.

If baseline procedures do not exist, not implemented reliably or not complete, this is a Finding.

Fixes: DB-DG0021-Generic (Manual)
Develop, document and implement baseline procedures that include all DBMS software files and directories.

Update the baseline after new installations, upgrades or maintenance activities that include changes to the software baseline.

Vulnerability Key: V0015610

STIG ID: DG0025

Release Number: 6

Status: Active

Short Name: DBMS encryption compliance

Long Name: DBMS should use NIST FIPS 140-2 validated cryptography.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	-------------------------------------	-------------------------------------	-------------------------------------

STIG ID: DG0025-Generic

Severity: Category II

**Severity
Override**

Guidance:

**Vulnerability
Discussion:** Use of cryptography to provide confidentiality and non-repudiation is not effective unless strong methods are employed with its use. Many earlier encryption methods and modules have been broken and/or overtaken by increasing computing power. The NIST FIPS 140-2 cryptographic standards provide proven methods and strengths to employ cryptography effectively.

**Default
Finding
Details:**

DBMS does not use NIST FIPS 140-2 validated cryptography.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCNR-1

Checks:

DB-DG0025-Generic (Manual)

If cryptography being used by the DBMS is not NIST FIPS 140-2 certified, this is a Finding.

Maintain a copy of the FIPS 140-2 Validation Certificate for the cryptographic modules in use as proof of certification.

Detailed information on the NIST Cryptographic Module Validation Program (CMVP) is available at the following website:

<http://csrc.nist.gov/groups/STM/cmvp/index.html>

--

Review the DBMS documentation to determine where cryptography may be used and/or configured.

Review network communication encryption options, data object encryption (both tables and application code objects), and encryption key management.

Where cryptography is employed and configured by the database, review the configuration settings to see if they use:

- 1) Compliant Algorithms - (AES (128, 192 or 256), Triple DES or TDEA (3 distinct 56-bit keys) , Skipjack)
- 2) Compliant Hash Functions - (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-5122)
- 3) Validated Cryptographic Modules - (whether native to the database or not)

Detailed information on the FIPS 140-2 standard is available at the following website:

<http://csrc.nist.gov/groups/SMA/index.html>

If non-compliant algorithms or hash functions are specified, this is a Finding.

If unvalidated cryptographic modules are in use, this is a Finding.

Fixes:

DB-DG0025-Generic (Manual)

Obtain and utilize native or third-party NIST FIPS 140-2 validated cryptography solution for the

DBMS.

Configure cryptographic functions to use FIPS 140-2 compliant algorithms and hashing functions.

Note: FIPS 140-2 compliance or non-compliance for the host and network is outside the purview of the Database STIG. FIPS 140-2 non-compliance at the host/network level does not negate this requirement.

Vulnerability Key: V0005685

STIG ID: DG0029

Release Number: 8

Status: Active

Short Name: Database auditing

Long Name: Required auditing parameters for database auditing should be set.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0029-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Auditing provides accountability for changes made to the DBMS configuration or its objects and data. It provides a means to discover suspicious activity and unauthorized changes. Without auditing, a compromise may go undetected and without a means to determine accountability.

Default Finding Details: Required auditing parameters for database auditing are not set.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-1, ECAR-2, ECAR-3

Checks: DB-DG0029-Generic (Manual)
 Review the audit setting for the database.

If auditing is not enabled, this is a Finding.

Fixes:

DB-DG0029-Generic (Manual)

Enable auditing on the database. If auditing is not provided natively with the DBMS, then obtain and implement a third-party DBMS audit tool. The tool must provide the minimum capability to audit required events (DG0141, DG0142, DG0145, DG0146).

Vulnerability Key: V0002507

STIG ID: DG0030

Release Number: 10

Status: Active

Short Name: DBMS audit data maintenance

Long Name: Audit trail data should be retained for one year.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0030-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures.

Default Finding Details: Audit trail data is not retained for one year.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECRR-1

Checks: DB-DG0030-Generic (Manual)
Review and verify the implementation of an audit trail retention policy.
Verify that audit data is maintained for a minimum of one year.

Fixes:

If audit data is not maintained for a minimum of one year, this is a Finding.

DB-DG0030-Generic (Manual)

Develop, document and implement an audit retention policy and procedures.

It is recommended that the most recent thirty days of audit logs remain available online.

After thirty days, the audit logs may be maintained offline.

Online maintenance provides for a more timely capability and inclination to investigate suspicious activity.

Vulnerability Key: V0015133

STIG ID: DG0031

Release Number: 9

Status: Active

Short Name: DBMS audit of changes to data

Long Name: Transaction logs should be periodically reviewed for unauthorized modification of data. Users should be notified of time and date of the last change in data content.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0031-Generic

Severity: Category II

Severity

Override

Guidance:

Vulnerability Discussion: Unauthorized or malicious changes to data compromise the integrity and usefulness of the data. Auditing changes to data supports accountability and non-repudiation. Auditing changes to data may be provided by the application accessing the DBMS or may depend upon the DBMS auditing functions. When DBMS auditing is used, the DBA is responsible for ensuring the auditing configuration meets the application design requirements.

Default Finding Details: Transaction logs are not periodically reviewed for unauthorized modification of data.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)

Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCD-1

Checks:

DB-DG0031-1-Generic (Interview)

If the application does not require auditing using DBMS features, this check is Not Applicable.

Review the application System Security Plan for requirements for database configuration for auditing changes to application data.

If the application requires DBMS auditing for changes to data, review the database audit configuration against the application requirement. If the auditing does not comply with the requirement, this is a Finding.

Fixes:

DB-DG0031-1-Generic (Manual)

Configure database data auditing to comply with the requirements of the application.

Document auditing requirements in the System Security Plan.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition:

Generic Database Installation (Target: Generic Database Installation)

Policy:

All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID:

DG0031-Generic

Severity:

Category II

Severity Override**Guidance:****Vulnerability Discussion:**

Unauthorized or malicious changes to data compromise the integrity and usefulness of the data. Auditing changes to data supports accountability and non-repudiation. Auditing changes to data may be provided by the application accessing the DBMS or may depend upon the DBMS auditing functions. When DBMS auditing is used, the DBA is responsible for ensuring the auditing configuration meets the application design requirements.

Default Finding Details:

Transaction logs are not periodically reviewed for unauthorized modification of data. Users are not notified of time and date of the last change in data content.

Documentable: No**Documentable Explanation:****Responsibility:** Database Administrator**References:**

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCD-2

Checks:

DB-DG0031-2-Generic (Interview)

If the application does not require auditing using DBMS features, this check is Not Applicable.

Review the application System Security Plan for requirements for database configuration for auditing changes to application data.

If the application requires DBMS auditing for changes to data, review the database audit configuration against the application requirement. If the auditing does not comply with the requirement, this is a Finding.

Review policy and procedures for reviewing access and changes to data.

If policy and procedures are not in place, this is a Finding.

If access and changes to data are not periodically reviewed or immediately reviewed on system security events, this is a Finding.

If mechanisms are not in place to notify users of time and date of the last change in data content, this is a Finding.

Fixes:

DB-DG0031-2-Generic (Manual)

Configure database data auditing to comply with the requirements of the application.

Document auditing requirements in the System Security Plan.

Develop, document and implement policy and procedures for reviewing access and changes to data periodically or immediately upon system security events.

Develop, document and implement mechanisms to notify users of time and date of the last change in data content.

Vulnerability Key: V0005686

STIG ID: DG0032

Release Number: 10

Status: Active

Short Name: DBMS audit record access

Long Name: Audit records should be restricted to authorized individuals.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0032-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Audit data is frequently targeted by malicious users as it can provide a means to detect their activity. The protection of the audit trail data is of special concern and requires restrictions to allow only the auditor and DBMS backup, recovery, and maintenance users access to it.

Default Finding Details: Audit records are not restricted to authorized individuals.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECTP-1

Checks: DB-DG0032-Generic (Manual)
Review file permissions to all files located in the DBMS audit log directory.

If any allow access to users not authorized as DBAs or auditors, this is a Finding.

Review database object access permissions to any audit log data stored in the database.

If any permissions are granted to users not authorized as DBAs or auditors, this is a Finding.

Fixes: DB-DG0032-Generic (Manual)
Modify audit file and database audit object access to authorized DBAs and auditors.

Vulnerability Key: V0002422

STIG ID: DG0040

Release Number: 13

Status: Active

Short Name: DBMS software owner account access

Long Name: The DBMS software installation account should be restricted to authorized users.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0040-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: DBA and other privileged administrative or application owner accounts are granted privileges that allow actions that can have a greater impact on database security and operation. It is especially important to grant access to privileged accounts to only those persons who are qualified and authorized to use them.

Default**Finding**

The DBMS software installation account is not restricted to authorized users.

Details:

Documentable: No

Documentable**Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks:

DB-DG0040-Generic (Interview)

Review procedures for controlling and granting access to use of the DBMS software installation account.

If access or use of this account is not restricted to the minimum number of personnel required or unauthorized access to the account has been granted, this is a Finding.

Fixes:

DB-DG0040-Generic (Manual)

Develop, document and implement procedures to restrict use and require logging of use of the DBMS software installation account.

Document authorized personnel and assignments in the System Security Plan.

Vulnerability Key: V0015110

STIG ID: DG0041

Release Number: 8

Status: Active

Short Name: DBMS installation account use logging

Long Name: Use of the DBMS installation account should be logged.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition:

Generic Database Installation (Target: Generic Database Installation)

Policy:

All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID:

DG0041-Generic

Severity: Category II

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** The DBMS installation account may be used by any authorized user to perform DBMS installation or maintenance. Without logging, accountability for actions attributed to the account is lost.

**Default
Finding
Details:** Use of the DBMS installation account is not logged.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0041-Generic (Interview)
Review and verify implementation of logging procedures defined for use of the DBMS software installation account.

If procedures for logging access to the DBMS are not present or are not being followed, this is a Finding.

Host system audit logs should be echoed or matched in the DBMS installation account usage log along with an indication of the person who accessed the account and an explanation for the access.

Fixes: DB-DG0041-Generic (Manual)
Develop, document and implement a logging procedure for use of the DBMS software installation account that provides accountability to individuals for any actions taken by the account.

Vulnerability Key: V0015111

STIG ID: DG0042

Release Number: 8

Status: Active

Short Name: DBMS software installation account use

Long Name: Use of the DBMS software installation account should be restricted to DBMS software installation, upgrade and maintenance actions.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0042-Generic

Severity: Category II

**Severity
Override
Guidance:**

Vulnerability Discussion: The DBMS software installation account is granted privileges not required for DBA or other functions. Use of accounts configured with excess privileges may result in unauthorized or unintentional compromise of the DBMS.

Default Finding Details: Use of the DBMS software installation account is not restricted to DBMS software installation, upgrade, and maintenance actions.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0042-Generic (Interview)

Review the logs for usage of the DBMS software installation account.

Interview personnel authorized to access the DBMS software installation account to ask how the account is used.

If any usage of the account is to support daily operations or DBA responsibilities, this is a Finding.

Fixes: DB-DG0042-Generic (Manual)

Develop, document and implement policy and train authorized users to restrict usage of the DBMS software installation account for DBMS software installation, upgrade and maintenance actions only.

Vulnerability Key: V0002423

STIG ID: DG0050

Release Number: 11

Status: Active

Short Name: DBMS software and configuration file monitoring

Long Name: Database software, applications and configuration files should be monitored to discover unauthorized changes.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0050-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Unmanaged changes that occur to the database software libraries or configuration can lead to unauthorized or compromised installations.

Default Finding Details: Database software, applications, and configuration files are not monitored to discover unauthorized changes.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSL-1

Checks: DB-DG0050-Generic (Interview)

Review monitoring procedures and implementation evidence to verify that monitoring of changes to database software libraries, related applications and configuration files is done.

Verify that the list of files, directories, and database application objects (procedures, functions and triggers) being monitored is complete.

If monitoring does not occur or is not complete, this is a Finding.

Fixes: DB-DG0050-Generic (Manual)

Develop, document and implement procedures to monitor for unauthorized changes to DBMS software libraries, related software application libraries and configuration files.

If a third-party automated tool is not employed, an automated job that reports file information on the directories and files of interest and compares them to the baseline report for the same will meet the requirement.

File hashes or checksums should be used for comparisons as file dates may be manipulated by malicious users.

Vulnerability Key: V0003808

STIG ID: DG0051

Release Number: 11

Status: Active

Short Name: Database job/batch queue monitoring

Long Name: Database job/batch queues should be reviewed regularly to detect unauthorized database job submissions.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding	Comments:
-------------------------------------------------------------------------	-----------

☐ Not Applicable
☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0051-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Unauthorized users may bypass security mechanisms by submitting jobs to job queues managed by the database to be run under a more privileged security context of the database or host system. These queues should be monitored regularly to detect any such unauthorized job submissions.

Default Finding Details: Database job/batch queues are not reviewed regularly to detect unauthorized database job submissions.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0051-Generic (Manual)

Review jobs scheduled to start automatically at system startup or run periodically during database operations.

If any jobs listed are not documented or not authorized, this is a Finding.

Review monitoring procedures for job queues and evidence of implementation.

If procedures for monitoring job queues are not documented, are not complete or are not implemented, this is a Finding.

Fixes: DB-DG0051-Generic (Manual)

Develop, document and implement procedures to monitor the database job queues for unauthorized job submissions.

Document or note authorized job submissions in the System Security Plan.

Vulnerability Key: V0003807

STIG ID: DG0052

Release Number: 11

Status: Active

Short Name: DBMS software access audit

Long Name: All applications that access the database should be logged in the DBMS audit trail where available.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0052-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Protections and privileges are designed within the database to correspond to access via authorized software. Use of unauthorized software to access the database could indicate an attempt to bypass established permissions. Reviewing the use of application software to the database can lead to discovery of unauthorized access attempts.

Default Finding Details: All applications that access the database are not logged in the audit trail.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAT-1, ECAT-2

Checks: DB-DG0052-Generic (Interview)

Review the DBMS audit trail to determine if the names [or unique identifiers] of applications used to connect to the database are included.

If an alternate method other than DBMS logging is authorized and implemented, review the audit trail to determine if the names [or unique identifiers] of applications used to connect to the database are included.

If application access to the DBMS is not being audited, this is a Finding.

If auditing does not capture the name [or unique identifier] of applications accessing the DBMS at a minimum, this is a Finding.

Fixes: DB-DG0052-Generic (Manual)

Modify auditing to ensure audit records include identification of applications used to access the DBMS.

Ensure auditing captures the name [or unique identifier] of applications accessing the DBMS at a minimum.

Develop or procure a 3rd-party solution where native DBMS logging is not employed or does not capture required information.

Vulnerability Key: V0003809

STIG ID: DG0053

Release Number: 10

Status: Active

Short Name: DBMS client connection definition file

Long Name: A single database connection configuration file should not be used to configure all database clients.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0053-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Many sites distribute a single client database connection configuration file to all site database users that contains network access information for all databases on the site. Such a file provides information to access databases not required by all users that may assist in unauthorized access attempts.

Default Finding Details: A single database connection configuration file is used to configure all database clients regardless of differing client access requirements.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAN-1

Checks: DB-DG0053-Generic (Interview)

Review procedures for providing database connection information to users/user workstations.

If procedures do not indicate or implement restrictions to connections required by the particular user, this is a Finding.

Fixes: DB-DG0053-Generic (Manual)

Develop, document and implement procedures to supply database connection information to those authorized for the user.

Note: This check is specific for the DBMS host system and not directed at client systems (client systems are included in the Application STIG / Checklist), however, detection of unauthorized client connections to the DBMS host system obtained through log files should be performed regularly and documented where authorized.

Vulnerability Key: V0015611

STIG ID: DG0054

Release Number: 7

Status: Active

Short Name: DBMS software access audit review

Long Name: The audit logs should be periodically monitored to discover DBMS access using unauthorized applications.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0054-Generic

Severity: Category III

Severity Override

Guidance:

Vulnerability Discussion: Regular and timely reviews of audit records increases the likelihood of early discovery of suspicious activity. Discovery of suspicious behavior can in turn trigger protection responses to minimize or eliminate a negative impact from malicious activity. Use of unauthorized application to access the DBMS may indicate an attempt to bypass security controls including authentication and data access or manipulation implemented by authorized applications.

Default Finding Details: The audit logs are not periodically monitored to discover DBMS access using unauthorized applications.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References:

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

ECAT-1, ECAT-2

Checks:

DB-DG0054-Generic (Interview)

Review procedures for and evidence of monitoring the audit log to detect access by unauthorized applications in the System Security Plan.

If the procedures or evidence does not exist, this is a Finding.

If alerts are not generated automatically, manual reviews should occur weekly or more frequently.

If evidence of manual reviews does not exist, this is a Finding.

Fixes:

DB-DG0054-Generic (Manual)

Develop, document and implement procedures for monitoring application access to the database to detect access meant to bypass security controls.

Where alerts are not implemented or available, establish weekly or more frequent review of queue activity.

Vulnerability Key: V0015120**STIG ID:** DG0064**Release Number:** 8**Status:** Active**Short Name:** DBMS backup and restoration file protection**Long Name:** DBMS backup and restoration files should be protected from unauthorized access.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0064-Generic**Severity:** Category II**Severity Override Guidance:**

Vulnerability Discussion: Lost or compromised DBMS backup and restoration files may lead to not only the loss of data, but also the unauthorized access to sensitive data. Backup files need the same protections against unauthorized access when stored on backup media as when online and actively in use by the database system. In addition, the backup media needs to be protected against physical loss. Most DBMSs maintain online copies of critical control files to provide transparent or easy recovery from hard disk loss or other interruptions to database operation.

Default Finding Details:

DBMS backup and restoration files are not protected from unauthorized access.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation COBR-1

Checks: DB-DG0064-Generic (Interview)

Review file protections assigned to online backup and restoration files.

Review access protections and procedures for offline backup and restoration files.

If backup or restoration files are subject to unauthorized access, this is a Finding.

It may be necessary to review backup and restoration procedures to determine ownership and access during all phases of backup and recovery.

In addition to physical and host system protections, consider other methods including password protection to the files.

Fixes: DB-DG0064-Generic (Manual)

Develop, document and implement protection for backup and restoration files.

Document personnel and the level of access authorized for each to the backup and restoration files in the System Security Plan.

Vulnerability Key: V0003810

STIG ID: DG0065

Release Number: 9

Status: Active

Short Name: DBMS PKI authentication

Long Name: DBMS authentication should require use of a DoD PKI certificate.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0065-Generic

Severity: Category II

**Severity
Override**

Guidance:

Vulnerability Discussion: In a properly configured DBMS, access controls defined for data access and DBMS management actions are assigned based on the user identity and job function. Unauthenticated or falsely authenticated access leads directly to the potential unauthorized access, misuse and lost accountability of data and activities within the DBMS. Use of PKI certificates for authentication to the DBMS provides a robust mechanism to ensure identity to authorize access to the DBMS.

Default

Finding Details: DBMS authentication does not require use of a DoD PKI certificate.

Documentable: No

Documentable**Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IATS-1, IATS-2

Checks: DB-DG0065-Generic (Interview)

If user access to the DBMS is via a portal or mid-tier system or product and PKI-authentication occurs at the portal/mid-tier, this check is Not a Finding.

Review the list of all DBMS accounts and their authentication methods.

This list is usually available from a system view or table and is easily gained from a simple SQL query.

If any accounts are listed with an authentication method other than a PKI certificate, this is a Finding.

For MAC 3 systems, if identification and authentication is not accomplished using the DoD PKI Class 3 certificate and hardware security token (when available) at minimum, this is a Finding.

For MAC 1 and 2 systems, if identification and authentication is not accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product at minimum, this is a Finding.

Fixes:

DB-DG0065-Generic (Manual)

Implement PKI authentication for all accounts defined within the database where applicable.

Applications may use host system (server) certificates to authenticate.

For MAC 3 systems, use of the DoD PKI Class 3 certificate and hardware security token (when available) at minimum is required.

For MAC 1 and 2 systems, use of the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product at minimum is required.

Vulnerability Key: V0003811

STIG ID: DG0066

Release Number: 9

Status: Active

Short Name: DBMS temporary password procedures

Long Name: Procedures for establishing temporary passwords that meet DoD password requirements for new accounts should be defined, documented and implemented.

Comments:

- ☐ Open
- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0066-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: New accounts authenticated by passwords that are created without a password or with an easily guessed password are vulnerable to unauthorized access. Procedures for creating new accounts with passwords should include the required assignment of a temporary password to be modified by the user upon first use.

Default Finding Details: Procedures for establishing temporary passwords that meet DoD password requirements for new accounts are not defined, documented or implemented.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0066-Generic (Interview)

If all DBMS accounts are configured to authenticate using certificates or other credential besides passwords, this check is Not a Finding.

Where accounts are authenticated using passwords, review procedures and implementation evidence for creation of temporary passwords.

If the procedures or evidence do not exist or do not enforce passwords to meet DoD password requirements, this is a Finding.

Fixes: DB-DG0066-Generic (Manual)

Develop, document and implement procedures for assigning temporary passwords to user accounts.

Procedures should include instruction to meet current DoD password length and complexity requirements and provide a secure method to relay the temporary password to the user.

Temporary passwords should also be short-lived and require immediate update by the user upon first login.

Vulnerability Key: V0003812

STIG ID: DG0067

Release Number: 11

Status: Active

Short Name: DBMS account password storage

Long Name: Database account passwords should be stored in encoded or encrypted format whether stored in database objects, external host files, environment variables or any other storage locations.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0067-Generic

Severity: Category I

Severity Override

Guidance:

Vulnerability Discussion: Database passwords stored in clear text are vulnerable to unauthorized disclosure. Database passwords should always be encoded or encrypted when stored internally or externally to the DBMS.

Default Finding Details: Database account passwords are not stored in encoded or encrypted format whether stored in database objects, external host files, environment variables or any other storage locations.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0067-Generic (Interview)

This check applies specifically to the Oracle DBMS installation and its associated files, scripts and environments.

This check does not apply to compiled, encoded or encrypted application source code and batch job code covered in Check DG0130.

Ask the DBA to review the list of DBMS database objects, database configuration files, associated scripts and applications defined within and external to the DBMS that access the database.

The list should also include files or settings used to configure the operational environment for the

DBMS and for interactive DBMS user accounts.

Ask the DBA and/or IAO to determine if any DBMS database objects, database configuration files, associated scripts and applications defined within or external to the DBMS that access the database, and DBMS / user environment files/settings contain database passwords.

If any do, confirm that DBMS passwords stored internally or externally to the DBMS are encoded or encrypted.

If any passwords are stored in clear text, this is a Finding.

If a list of DBMS database objects, database configuration files, associated scripts and applications defined within or external to the DBMS that access the database, and DBMS / user environment files/settings is not maintained in the System Security Plan, this is a Finding.

Fixes:

DB-DG0067-Generic (Manual)

Develop, document and maintain a list of DBMS database objects, database configuration files, associated scripts and applications defined within or external to the DBMS that access the database, and DBMS / user environment files/settings in the System Security Plan.

Record whether they do or do not contain DBMS passwords.

If passwords are present, ensure they are encoded or encrypted and protected by host system security.

Consider using vendor or 3rd party tools to support external authentication.

Vulnerability Key: V0003813

STIG ID: DG0068

Release Number: 10

Status: Active

Short Name: DBMS application password display

Long Name: DBMS tools or applications that echo or require a password entry in clear text should be protected from password display.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0068-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Database applications may allow for entry of the account name and password as a visible parameter of the application execution command. This practice should be prohibited and disabled, if possible, by the application. If it cannot be disabled, users should be strictly instructed not to use this feature. Typically, the application will prompt for this information and accept it without echoing it on the users computer screen.

Default Finding Details: DBMS tools or applications that echo or require a password entry in clear text are not protected from password display.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0068-Generic (Interview)
Interview the DBA to determine if any applications that access the database (i.e. sqlcmd, sqlplus, etc.) allow for entry of the account name and password on the command line.

If any applications exist and are in use, ask the DBA if users have been instructed not to include passwords on the command line and if these applications are monitored for compliance.

If documentation of instruction and monitoring are not being performed, this is a Finding.

Fixes: DB-DG0068-Generic (Manual)
Configure or modify applications to prohibit display of passwords in clear text on the command line if possible.

Implement policy and train users to prohibit entry of passwords on the command line for applications that cannot be modified or configured to deny this.

Remove any applications that can access the database if they are not being used or cannot be monitored.

Vulnerability Key: V0015140

STIG ID: DG0069

Release Number: 8

Status: Active

Short Name: Production data import to development DBMS

Long Name: Procedures and restrictions for import of production data to development databases should be documented, implemented and followed.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC /

	I - Mission Critical	II - Mission Support	III - Administrative
--	----------------------	----------------------	----------------------

Confidentiality Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0069-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Data export from production databases may include sensitive data. Application developers do not have a need to know sensitive data. Any access they may have to production data would be considered unauthorized access and subject the sensitive data to unlawful or unauthorized disclosure.

Default Finding Details: Procedures and restrictions for import of production data to development databases are not documented, implemented or followed.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAN-1

Checks: DB-DG0069-Generic (Interview)

If the database being reviewed is not a production database, this check is Not Applicable.

Review procedures or restrictions for data exports from the production database.

If data exports are not allowed, then review methods for preventing and monitoring of any production data export.

If procedures and methods are not complete or implemented, this is a Finding.

Acknowledgement of data export restrictions and procedures by individuals granted privileges that enable data export is considered sufficient protection, however, record of such acknowledgement must be filed.

Privileges required for database copy and/or export commands include sysadmin, DATABASE CREATOR or database owner of the source database.

If DBMS export utilities are not restricted to users authorized by the IAO, this is a Finding.

Fixes: DB-DG0069-Generic (Manual)

Document procedures and restrictions for production data export.

Require any users assigned privileges that allow the export of production data from the database to acknowledge understanding of the export restrictions.

Restrict permissions allowing use or access to database export procedures or functions to authorized users.

Vulnerability Key: V0015612

STIG ID: DG0072

Release Number: 4

Status: Active
Short Name: DBMS Password change time limit
Long Name: Database password changes by users should be limited to one change within 24 hours where supported by the DBMS.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0072-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Frequent password changes may indicate suspicious activity or attempts to bypass password controls based on password histories. Limiting the frequency of password changes helps to enforce password change rules and can lead to the discovery of compromised accounts.

Default Finding Details: Database password changes by users are not limited to one change within 24 hours where supported by the DBMS.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0072-Generic (Manual)

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

If the DBMS does not natively support this functionality, this check is Not a Finding.

If the DBMS supports this functionality, review the settings and function logic or have the DBA demonstrate a password change to ensure that the function does not allow user changes to passwords to occur more than once within a 24-hour period.

If the review or the demonstration reveals that passwords can be changed by users more than once within a 24-hour period, this is a Finding.

Fixes: DB-DG0072-Generic (Manual)

Define, configure and test a password verify feature or function that authenticates passwords on change to ensure that changes to passwords do not occur more than once within a 24-hour period.

Vulnerability Key: V0003819

STIG ID: DG0076

Release Number: 11

Status: Active

Short Name: Sensitive data import to development DBMS

Long Name: Sensitive information from production database exports should be modified after import to a development database.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0076-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Data export from production databases may include sensitive data. Application developers do not have a need to know to sensitive data. Any access they may have to production data would be considered unauthorized access and subject the sensitive data to unlawful or unauthorized disclosure. See DODD 8500.1 for a definition of Sensitive Information.

Default Finding Details: Sensitive information from production database exports remains unmodified after import to a development database.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAN-1

Checks: DB-DG0076-Generic (Interview)

If database exports are not generated for import on development systems from production databases containing sensitive information as determined by the Information Owner, this check is Not Applicable.

Review procedures and restrictions for data exports from production databases.

If data exports are allowed, review procedures for protecting any sensitive data included in the exports.

If sensitive data is included in the exports and no protections are taken to remove or modify the

data to render it not sensitive (when provided to admins, users or systems that do not have clearance to access the sensitive information), this is a Finding.

Fixes:

DB-DG0076-Generic (Manual)

Develop, document and implement procedures and restrictions for production data export.

Require any users assigned privileges that allow the export of production data from the database to acknowledge understanding of the export restrictions.

Restrict permissions allowing use or access to database export procedures or functions to authorized users.

Apply documented procedures to remove or alter sensitive information from production database exports when importing into development databases.

Vulnerability Key: V0003820

STIG ID: DG0077

Release Number: 11

Status: Active

Short Name: Production data protection on a shared system

Long Name: Production databases should be protected from unauthorized access by developers on shared production/development host systems.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0077-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Developers granted elevated database, operating system privileges on systems that support both development, and production databases can affect the operation and/or security of the production database system. Operating system and database privileges assigned to developers on shared development and production systems should be restricted.

Default Finding Details: Production databases are not protected from unauthorized access by developers on shared production/development host systems.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0077-Generic (Interview)

Review the list of instances and databases installed on the host system with the DBA.

Ask which databases are production databases and which are for development.

If only development or only production databases exist on this host, this is Not a Finding.

Otherwise, ask the DBA to confirm that policy and procedures are in place for the IAO to review database and operating system privileges on the system.

If none is in place, this is a Finding.

Ask the DBA/SA if developer host accounts have been granted privileges to production database directories, files or resources.

If they have been, this is a Finding.

NOTE: Though shared production/non-production DBMS installations was allowed under previous database STIG guidance, doing so may place it in violation of OS, Application, Network or Enclave STIG guidance. Ensure that any shared production/non-production DBMS installations meets STIG guidance requirements at all levels or mitigate any conflicts in STIG guidance with your DAA.

Fixes: DB-DG0077-Generic (Manual)

Develop, document and implement procedures to review and maintain privileges granted to developers on shared production and development host systems and databases.

Recommend establishing a dedicated DBMS host for production DBMS installations (See Checks DG0109 and DG0110).

A dedicated host system in this case refers to an instance of the operating system at a minimum.

The operating system may reside on a virtual host machine where supported by the DBMS vendor.

Vulnerability Key: V0015613

STIG ID: DG0078

Release Number: 5

Status: Active

Short Name: DBMS individual accounts

Long Name: Each database user, application or process should have an individually assigned account.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC /

--	--	--	--

Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0078-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Use of accounts shared by multiple users, applications, or processes limit the accountability for actions taken in or on the data or database. Individual accounts provide an opportunity to limit database authorizations to those required for the job function assigned to each individual account.

Default Finding Details: Each database user, application, or process does not have an individually assigned account.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0078-Generic (Manual)
Review DBMS account names against the list of authorized DBMS accounts in the System Security Plan.

If any accounts indicate use by multiple persons that are not mapped to a specific person, this is a Finding.

If any applications or processes share an account that could be assigned an individual account or are not specified as requiring a shared account, this is a Finding.

Note: Privileged installation accounts may be required to be accessed by DBA or other administrators for system maintenance.

In these cases, each use of the account must be logged in some manner to assign accountability for any actions taken during the use of the account.

Fixes: DB-DG0078-Generic (Manual)
Create individual accounts for each user, application, or other process that requires a database connection.

Document any accounts that are shared where separation is not supported by the application or for maintenance support.

Design, develop and implement a method to log use of any account to which more than one person has access. Restrict interactive access to shared accounts to the fewest persons possible.

Vulnerability Key: V0015102

STIG ID: DG0083

Release Number: 8

Status: Active
Short Name: DBMS audit report automation
Long Name: Automated notification of suspicious activity detected in the audit trail should be implemented.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0083-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Audit record collection may quickly overwhelm storage resources and an auditor's ability to review it in a productive manner. Automated tools can provide the means to manage the audit data collected as well as present it to an auditor in an efficient way.

Default Finding Details: Automated notification of suspicious activity detected in the audit trail is not implemented.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECRG-1

Checks: DB-DG0083-Generic (Interview)
 Review automated tool usage for reporting of audit trail data.
 If automated tools are not used, this is a Finding.

Automated DBMS jobs and/or procedures may be used to produce the periodic reports.

Fixes: DB-DG0083-Generic (Manual)
 Develop, document and implement database or host system procedures to report audit trail data in a form usable to detect unauthorized access to or usage of DBMS privileges, procedures or data.

Vulnerability Key: V0015614

STIG ID: DG0084

Release Number: 4

Status: Active
Short Name: DBMS residual data clearance
Long Name: The DBMS should be configured to clear residual data from memory, data objects and files, and other storage locations.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0084-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Database storage locations may be reassigned to different objects during normal operations. If not cleared of residual data, sensitive data may be exposed to unauthorized access.

Default Finding Details: The DBMS is not configured to clear residual data from memory, data objects or files, or other storage locations.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECRC-1

Checks: DB-DG0084-Generic (Manual)
 Determine if any options are available to clear residual data from storage locations after use.
 Look for options to clear memory locations, data object storage, or host system data files.
 If options are not available, this check is Not Applicable.
 If options are available, but not employed, this is a Finding.

Fixes: DB-DG0084-Generic (Manual)
 Configure all available options to clear storage locations of residual data, including options to clear memory locations, data object storage and host system data files.

Vulnerability Key: V0015615

STIG ID: DG0085

Release Number: 4

Status: Active

Short Name: Minimum DBA privilege assignment

Long Name: The DBA role should not be assigned excessive or unauthorized privileges.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0085-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The default DBA privileges typically include all privileges defined for a DBMS. These privileges are required to configure the DBMS and to provide other users access to DBMS objects. However, DBAs may not require access to application data or other privileges to administer the DBMS. Where not required or desired, DBAs may be prevented from accessing protected data for which they have no need-to-know or from utilizing unauthorized privileges for other actions. Although DBAs may assign themselves privileges to override any restrictions, the assignment of privileges is an audit requirement and this auditable event may assist discovery of a misuse of privileges.

Default Finding Details:

The DBA role is assigned excessive or unauthorized privileges.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks: DB-DG0085-Generic (Interview)

Review privileges assigned to the DBA roles and compare them to those listed in the System Security Plan with the IAO.

If privileges are granted to DBAs that are not listed as required privileges in the System Security Plan, this is a Finding.

Note: If the number of DBAs appears excessive to for the same job function, then query the DBA to discover if separating DBA roles by specific job function is in order.

Query the DBA or IAO to determine the advisability of having only one DBA job function defined.

If security would be enhanced by separating DBA responsibilities into separate job functions with custom DBA roles, this is Not a Finding.

Fixes:

DB-DG0085-Generic (Manual)
Limit privileges assigned to DBA roles.

Document DBA job functions and minimum privileges required to perform the DBA job function in the System Security Plan.

Where many DBAs administer the same DBMS, consider dividing DBA job functions to restrict DBAs to administering a smaller portion of the DBMS to prevent intentional or inadvertent modification to the entire DBMS or specific portions.

Vulnerability Key: V0015112

STIG ID: DG0088

Release Number: 8

Status: Active

Short Name: DBMS vulnerability mgmt and IA compliance testing

Long Name: The DBMS should be periodically tested for vulnerability management and IA compliance.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0088-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: The DBMS security configuration may be altered either intentionally or unintentionally over time. The DBMS may also be the subject of published vulnerabilities that require the installation of a security patch or a reconfiguration to mitigate the vulnerability. If the DBMS is not monitored for required or unintentional changes that render it not compliant with requirements, it can be vulnerable to attack or compromise.

Default Finding Details: The DBMS is not periodically tested for vulnerability management and IA compliance.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)

Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
 ECMT-1, ECMT-2

Checks:

DB-DG0088-Generic (Interview)

Review procedures and evidence of implementation for DBMS IA and vulnerability management compliance.

This should include periodic, unannounced, in-depth monitoring and provide for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled and conducted.

Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

The results for Classified systems are required to be independently validated.

If the requirements listed above are not being met, this is a Finding.

Fixes:

DB-DG0088-Generic (Manual)

Develop, document and implement procedures for periodic testing of the DBMS for current vulnerability management and security configuration compliance as stated in the check.

Coordinate 3rd-party validation testing for Classified systems.

Vulnerability Key: V0015131

STIG ID: DG0090

Release Number: 7

Status: Active

Short Name: DBMS sensitive data identification and encryption

Long Name: Sensitive information stored in the database should be protected by encryption.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0090-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Sensitive data stored in unencrypted format within the database is vulnerable to unauthorized viewing.

Default

Finding Details: Sensitive information stored in the database is not protected by encryption.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCR-1, ECCR-2, ECCR-3

Checks: DB-DG0090-Generic (Manual)
If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

Ask the DBA to use select statements in the database to review sensitive data stored in tables as identified in the System Security Plan and/or AIS Functional Architecture documentation.

If any sensitive data is human readable by unauthorized users, this is a Finding.

If encryption is required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.

If encryption is required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-sources and methods intelligence information.

If a classified enclave contains sources and methods intelligence data and is accessed by individuals lacking an appropriate clearance for sources and methods intelligence, then NSA-approved cryptography is used to encrypt all sources and methods intelligence stored within the enclave.

Fixes: DB-DG0090-Generic (Manual)
Use third-party tools or native DBMS features to encrypt sensitive or classified data stored in the database.

Use only NIST-certified or NSA-approved cryptography to provide encryption.

Document acceptance of risk by the Information Owner where sensitive or classified data is not encrypted.

Have the IAO document assurance that the unencrypted sensitive or classified information is otherwise inaccessible to those who do not have Need-to-Know access to the data.

Developers should consider using a record-specific encryption method to protect individual records.

For example, by employing the session username or other individualized element as part of the encryption key, then decryption of a data element is only possible by that user or other data accessible only by that user.

Consider applying additional auditing of access to any unencrypted sensitive or classified data when accessed by users (with and/or without Need-to-Know).

STIG ID: DG0092
Release Number: 10
Status: Active
Short Name: DBMS data file encryption
Long Name: Database data files containing sensitive information should be encrypted.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0092-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Where system and DBMS access controls do not provide complete protection of sensitive or classified information, the Information Owner may require encryption to provide additional protection. Encryption of sensitive data helps protect disclosure to privileged users who do not have a need-to-know requirement to the data, but may be able to access DBMS data files using OS file tools.

Default Finding Details:

Database data files containing sensitive information are not encrypted.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCR-1, ECCR-2, ECCR-3

Checks: DB-DG0092-Generic (Manual)

Review the System Security Plan and/or the AIS Functional Architecture documentation to discover sensitive or classified data identified by the Information Owner that requires encryption.

If no sensitive or classified data is identified as requiring encryption by the Information Owner, this check is Not a Finding.

Have the DBA use select statements in the database to review sensitive data stored in tables as identified in the System Security Plan and/or AIS Functional Architecture documentation.

If all sensitive data as identified is encrypted within the database objects, encryption of the DBMS data files is optional and Not a Finding.

If all sensitive data is not encrypted within database objects, review encryption applied to the

DBMS host data files.

If no encryption is applied, this is a Finding.

If encryption is required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.

If encryption is required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-sources and methods intelligence information.

If a classified enclave contains sources and methods intelligence data and is accessed by individuals lacking an appropriate clearance for sources and methods intelligence, then NSA-approved cryptography is used to encrypt all sources and methods intelligence stored within the enclave.

Determine which DBMS data files contain sensitive data. Not all DBMS data files will require encryption.

Fixes:

DB-DG0092-Generic (Manual)

Use third-party tools or native DBMS features to encrypt sensitive or classified data stored in the database.

Use only NIST-certified or NSA-approved cryptography to provide encryption.

Document acceptance of risk by the Information Owner where sensitive or classified data is not encrypted.

Have the IAO document assurance that the unencrypted sensitive or classified information is otherwise inaccessible to those who do not have Need-to-Know access to the data.

To lessen the impact on system performance, separate sensitive data where file encryption is required into dedicated DBMS data files.

Consider applying additional auditing of access to any unencrypted sensitive or classified data when accessed by users (with and/or without Need-to-Know).

Vulnerability Key: V0003825

STIG ID: DG0093

Release Number: 9

Status: Active

Short Name: Remote administrative connection encryption

Long Name: Remote administrative connections to the database should be encrypted.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
STIG ID:	DG0093-Generic			
Severity:	Category II			
Severity Override Guidance:				
Vulnerability Discussion:	Communications between a client and database service across the network may contain sensitive information including passwords. This is particularly true in the case of administrative activities. Encryption of remote administrative connections to the database ensures confidentiality of configuration, management, and other administrative data.			
Default Finding Details:	Remote administrative connections to the database are not encrypted.			
Documentable:	No			
Documentable Explanation:				
Responsibility:	Database Administrator			
References:	Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8) Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCT-1, ECCT-2			
Checks:	<p>DB-DG0093-Generic (Interview)</p> <p>If no administration accounts are accessed remotely, this check is Not a Finding.</p> <p>Ask the DBA if access to the administration accounts is:</p> <ol style="list-style-type: none"> 1. Made using remote access through a local host account 2. Made directly to the database from a remote database client <p>If access is via a local host account, review procedures, policy, and/or evidence that remote administrative account access is performed only via an encrypted connection protocol such as SSH, Remote Desktop Connection (properly configured, of course), etc., to connect to the host.</p> <p>If it is not, this is a Finding.</p> <p>If access is via direct connection to the DBMS from a DBMS client, confirm that a dedicated database listener exists on the DBMS server and configured to encrypt communications for remote administrative connections.</p> <p>If it is not, this is a Finding.</p> <p>If there are any listeners on the DBMS host that are configured to accept unencrypted traffic, determine through review of policy and training evidence that DBAs know to use the encrypted listener for remote access to administrative accounts.</p> <p>If no such policy exists, the DBAs have not been instructed to use or do not use an encrypted connection, this is a Finding.</p> <p>Interview DBAs to confirm they use the encrypted listener for remote DBA access.</p> <p>If any DBAs do not, this is a Finding.</p> <p>Ensure unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.</p>			
Fixes:	<p>DB-DG0093-Generic (Manual)</p> <p>Do not administer DBMS systems remotely if possible.</p> <p>If this is not possible, ensure that all connections to the DBMS for administrative purposes utilize</p>			

encryption at all possible levels [i.e. Network (VPN), Host (SSH/RDP), and Database (Client/ODBC/listener)].

Ensure unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.

Vulnerability Key: V0003827

STIG ID: DG0095

Release Number: 11

Status: Active

Short Name: DBMS audit trail data review

Long Name: Audit trail data should be reviewed daily or more frequently.

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0095-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Review of audit trail data provides a means for detection of unauthorized access or attempted access. Frequent and regularly scheduled reviews ensures that such access is discovered in a timely manner.

Default Finding Details: Audit trail data is not reviewed daily or more frequently.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAT-1

Checks: DB-DG0095-Generic (Interview)
Review policy, procedures and implementation evidence for daily audit trail monitoring.

If the policy, procedures and evidence are not present or complete, this is a Finding.

Fixes: DB-DG0095-Generic (Manual)

Develop, document and implement policy and procedures to monitor audit trail data daily.

Vulnerability Key: V0015138

STIG ID: DG0096

Release Number: 8

Status: Active

Short Name: DBMS IA policy and procedure review

Long Name: The DBMS IA policies and procedures should be reviewed annually or more frequently.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0096-Generic

Severity: Category III

Severity Override

Guidance:

Vulnerability Discussion: A regular review of current database security policies and procedures is necessary to maintain the desired security posture of the DBMS. Policies and procedures should be measured against current DOD policy, STIG guidance, vendor-specific guidance and recommendations, and site-specific or other security policy.

Default Finding

The DBMS IA policies and procedures are not reviewed annually or more frequently.

Details:

Documentable: No

Documentable

Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCAR-1

Checks: DB-DG0096-Generic (Interview)

Review policy, procedures and implementation evidence of annual reviews of DBMS IA policy and procedures.

If policy and procedures do not exist, are incomplete, or are not implemented and followed annually or more frequently, this is a Finding.

Fixes: DB-DG0096-Generic (Manual)

Develop, document and implement policy and procedures to review DBMS IA policies and procedures on an annual or more frequent basis.

Vulnerability Key: V0015139

STIG ID: DG0097

Release Number: 8

Status: Active

Short Name: DBMS testing plans and procedures

Long Name: Plans and procedures for testing DBMS installations, upgrades, and patches should be defined and followed prior to production implementation.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0097-Generic

Severity: Category II

Severity

Override

Guidance:

Vulnerability Discussion: Updates and patches to existing software have the intention of improving the security or enhancing or adding features to the product. However, it is unfortunately common that updates or patches can render production systems inoperable or even introduce serious vulnerabilities. Some updates also set security configurations back to unacceptable settings that do not meet security requirements. For these reasons, it is a good practice to test updates and patches offline before introducing them in a production environment.

Default Finding Details: Plans and procedures for testing DBMS installations, upgrades and patches are not defined or followed prior to production implementation.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCCT-1

Checks: DB-DG0097-Generic (Interview)

Review policy and procedures for testing DBMS installations, upgrades and patches prior to production deployment.

If policy and procedures do not exist or evidence of implementation does not exist, this is a Finding.

Fixes: DB-DG0097-Generic (Manual)
Develop, document and implement policy and procedures for testing DBMS installations, upgrades and patches prior to deployment on production systems.

Vulnerability Key: V0015617

STIG ID: DG0098

Release Number: 4

Status: Active

Short Name: DBMS access to external local objects

Long Name: Access to external objects should be disabled if not required and authorized.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0098-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Objects defined within the database, but stored externally to the database are accessible based on authorizations defined by the local operating system or other remote system that may be under separate security authority. Access to external objects may thus be uncontrolled or not based on least privileges defined for each user job function. This in turn may provide unauthorized access to the external objects.

Default Finding Details: Access to external objects has not been disabled and is not required or authorized.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0098-Generic (Manual)
Review the database for definitions of application objects stored externally to the database.

Determine if there are methods to disable use or access or to remove definitions for external data objects.

If there are methods to prevent access to unused and unneeded external application data objects or the requirement for their use is not documented in the AIS functional architecture, this is a Finding.

Fixes:

DB-DG0098-Generic (Manual)

Include any external application data objects defined in the database that are required for authorized application use in the AIS functional architecture documentation.

Disable use of or remove any external application data object definitions that are not authorized.

Vulnerability Key: V0015618

STIG ID: DG0099

Release Number: 4

Status: Active

Short Name: DBMS access to external local executables

Long Name: Access to external DBMS executables should be disabled or restricted.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0099-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: DBMS's may spawn additional external processes to execute procedures that are defined in the DBMS, but stored in external host files (external procedures). The spawned process used to execute the external procedure may operate within a different OS security context than the DBMS and provide unauthorized access to the host system.

Default Finding Details:

Access to external DBMS executables is not disabled or restricted.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)

Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks:

DB-DG0099-Generic (Manual)

Review the database for definitions of application executable objects stored externally to the database.

Determine if there are methods to disable use or access or to remove definitions for external executable objects.

Verify that any application executable objects listed have their use documented in the AIS Functional Architecture documentation as required for operation and authorized by the IAO.

If any are not, this is a Finding.

Fixes:

DB-DG0099-Generic (Manual)

Include any external application executable objects defined in the database that are required for authorized application use in the AIS functional architecture documentation.

Disable use of or remove any external application executable object definitions that are not authorized.

Vulnerability Key: V0015620

STIG ID: DG0101

Release Number: 4

Status: Active

Short Name: DBMS external procedure OS account privileges

Long Name: OS accounts used to execute external procedures should be assigned minimum privileges.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0101-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: External applications spawned by the DBMS process may be executed under OS accounts assigned unnecessary privileges that can lead to unauthorized access to OS resources. Unauthorized access to OS resources can lead to the compromise of the OS, the DBMS, and any other service provided by the host platform.

Default

Finding Details: OS accounts used to execute external procedures are not assigned minimum privileges.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0101-Generic (Manual)

Determine which OS accounts external DBMS executables are run.

Review the privileges assigned to these accounts and compare them to the System Security Plan and the function of the applications.

If assigned privileges exceed those necessary to operate as designed or the privileges do not match the list of required privileges for the application in the System Security Plan, this is a Finding.

Fixes: DB-DG0101-Generic (Manual)

Configure OS accounts used by DBMS external procedures to have the minimum privileges necessary for operation.

Document DBMS external procedures and OS privileges need to execute the procedures in the System Security Plan.

Vulnerability Key: V0015141

STIG ID: DG0102

Release Number: 7

Status: Active

Short Name: DBMS services dedicated custom account

Long Name: DBMS processes or services should run under custom, dedicated OS accounts.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0102-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Shared accounts do not provide separation of duties nor allow for assignment of least privileges for use by database processes and services. Without separation and least privilege, the exploit of one service or process is more likely to be able to compromise another or all other services.

Default

Finding Details: DBMS processes or services are not run under custom, dedicated OS accounts.

Documentable: No

Documentable**Explanation:**

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0102-Generic (Manual)

Review the list of DBMS processes and/or services running on the host system and compare to the vendor documentation on the DBMS supporting processes/services.

For any process or service related to the DBMS, view the process or service account that owns the related executable or under which the executable runs.

If any of the processes or services do not use a custom account and are not explicitly required by the vendor to share the same account as one of the other DBMS processes or services, this is a Finding.

If any of the DBMS processes or services use a domain user account on a Windows host, then review the requirement for the domain user account.

If the service does not require interaction with network or domain resources, this is a Finding.

Note: Use of a local Windows user account is recommended unless domain or network resources are accessed by the service.

For Windows:

Review user rights assigned to any DBMS process or service accounts. User rights may be assigned to the service accounts via Windows groups or group policies.

If any Windows user rights other than those listed as the minimum required in vendor documentation are assigned to the service accounts, this is a Finding.

For UNIX:

Review ownership of and permissions assigned to DBMS process executables.

If the owner account is not dedicated for the process, group membership is unnecessarily shared, or other permissions not required for operation are assigned, this is a Finding.

Fixes:

DB-DG0102-Generic (Manual)

Create and assign custom user accounts for the individual DBMS process or services to use where supported by the DBMS.

Disable any DBMS process or service accounts not required for operation.

Assign only required user rights or privileges to the custom service accounts or process executables.

Document assignments in the System Security Plan.

Vulnerability Key: V0015621

STIG ID: DG0103

Release Number: 6

Status: Active

Short Name: DBMS Listener network restrictions

Long Name: The DBMS listener should restrict database access by network address.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0103-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Network listeners provide the means to connect to the DBMS from remote systems. Restricting remote access to specific, trusted systems helps prevent access by unauthorized and potentially malicious users.

Default Finding Details: The DBMS listener does not restrict database access by network address.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0103-Generic (Manual)

Review the DBMS network communication architecture. If the DBMS does not provide a native network listening component, this check is Not a Finding.

Review the network configuration options.

If the configuration does not provide a means to restrict access by network address, this check is Not a Finding.

If a capability to restrict network access is provide by the DBMS listener, then review the restrictions listed.

If they do not adequately restrict access or do not meet the required restrictions as documented in the System Security Plan, this is a Finding.

Fixes: DB-DG0103-Generic (Manual)

Configure available DBMS network listening components to restrict access to the DBMS by network address.

Document in the System Security Plan the list of remote systems and their network addresses that are allowed access to the DBMS.

The list need not include details where the number of remote systems is large, but should include remote systems by subnet at a minimum.

Vulnerability Key: V0015622

STIG ID: DG0104

Release Number: 7

Status: Active

Short Name: DBMS service identification

Long Name: DBMS service identification should be unique and clearly identifies the service.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0104-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Local or network services that do not employ unique or clearly identifiable targets can lead to inadvertent or unauthorized connections.

Default Finding Details: DBMS service identification is not unique or does not clearly identify the service.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0104-Generic (Manual)

Review the DBMS process or service names advertised or displayed by the DBMS.

If multiple DBMS service or process names are listed and do not clearly identify the use of the service/process or clearly differentiate them from one another, this is a Finding.

An example of service/process naming that meets the requirement: prdinv01, dvsales02, msfindb1.

An example of service/process naming that does not meet the requirement: Instance1, MyInstance, SQL7, orcl.

It may be necessary to interview the DBA for an understanding of the naming scheme to determine if the names provide clear differentiations to themselves and remote users.

Fixes:

DB-DG0104-Generic (Manual)

Create process names that provide a clear differentiation of purpose of the database or database instance and does not identify the product version.

Follow vendor documentation to change the service or process names.

Vulnerability Key: V0015144

STIG ID: DG0107

Release Number: 8

Status: Active

Short Name: DBMS sensitive data identification

Long Name: Sensitive data is stored in the database and should be identified in the System Security Plan and AIS Functional Architecture documentation.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0107-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: A DBMS that does not have the correct confidentiality level identified or any confidentiality level assigned stands the chance of not being secured at a level appropriate to the risk it poses.

Default Finding Details: Sensitive data is stored in the database and is not identified in the System Security Plan and AIS Functional Architecture documentation.

Documentable: No

Documentable**Explanation:****Responsibility:** Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0107-Generic (Manual)

Review the System Security Plan and AIS Functional Architecture documentation for the DBMS and note any sensitive data that is identified.

Review database table column data or descriptions that indicate sensitive data.

For example, a data column labeled "SSN" could indicate social security numbers are stored in the column.

Question the IAO or DBA where any questions arise.

General categories of sensitive data requiring identification include any personal identifiable information (PII) involving health, financial and security proprietary or sensitive business data or data that might be classified.

If any columns in the database contain data considered sensitive and is not referenced in the System Security Plan and AIS Functional Architecture documentation, this is a Finding.

Fixes: DB-DG0107-Generic (Manual)

Include identification of any sensitive data in the System Security Plan and AIS Functional Architecture.

Include discussions of data that appear to be sensitive and annotate why it is not marked as such.

Vulnerability Key: V0015145**STIG ID:** DG0108**Release Number:** 8**Status:** Active**Short Name:** DBMS restoration priority**Long Name:** The DBMS restoration priority should be assigned.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)**Policy:** All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0108-Generic

Severity: Category III

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** When DBMS service is disrupted, the impact it has on the overall mission of the organization can be severe. Without the proper assignment of the priority to be placed on restoration of the DBMS and its subsystems, restoration of DBMS services may not meet mission requirements.

**Default
Finding
Details:** The DBMS restoration priority has not been assigned.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0108-Generic (Manual)
Review the System Security Plan to discover the restoration priority assigned to the DBMS.

If it is not assigned, this is a Finding.

Fixes: DB-DG0108-Generic (Manual)
Review the mission criticality of the DBMS in relation to the overall mission of the organization and assign it a restoration priority.

Vulnerability Key: V0015146

STIG ID: DG0109

Release Number: 8

Status: Active

Short Name: DBMS dedicated host

Long Name: The DBMS should not be operated without authorization on a host system supporting other application services.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0109-Generic

Severity: Category II

Severity**Override****Guidance:****Vulnerability****Discussion:**

In the same way that added security layers can provide a cumulative positive effect on security posture, multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system. A DBMS not installed on a dedicated host may pose a threat to and be threatened by other hosted applications. Applications that share a single DBMS may also create risk to one another. Access controls defined for one application by default may provide access to the other application's database objects or directories. Any method that provides any level of separation of security context assists in the protection between applications.

Default**Finding****Details:**

The DBMS is operated without authorization on a host system supporting other application services.

Documentable: No**Documentable****Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPA-1

Checks:

DB-DG0109-Generic (Manual)

Review the list of processes/services running on the DBMS host system.

For Windows, review the Services snap-in. For UNIX, review the processes using the ps command.

Investigate with the DBA/SA any unknown services.

If any of the services or processes are identified as supporting applications or functions not authorized in the System Security Plan, this is a Finding.

Note: Only applications that are operationally required to share the same host system may be authorized to do so.

Applications that share the same host for administrative, financial or other non-operational reasons may not be authorized and are a Finding.

Fixes:

DB-DG0109-Generic (Manual)

A dedicated host system in this case refers to an instance of the operating system at a minimum.

The operating system may reside on a virtual host machine if supported by the DBMS vendor.

Remove any unauthorized processes or services and install on a separate host system.

Where separation is not supported, update the System Security Plan and provide the technical requirement for having the application share a host with the DBMS.

Vulnerability Key: V0015179

STIG ID: DG0110

Release Number: 8

Status: Active

Short Name: DBMS host shared with a security service

Long Name: The DBMS should not share a host supporting an independent security service.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0110-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The Security Support Structure is a security control function or service provided by an external system or application. An example of this would be a Windows domain controller that provides identification and authentication that can be used by other systems to control access. The vulnerabilities and, therefore, associated risk of a DBMS installed on a system that provides a security support structure is significantly higher than when installed with other functions that do not provide security support. In cases where the DBMS is dedicated to local support of a security support function (e.g. a directory service), separation may not be possible.

Default Finding Details: The DBMS shares a host supporting an independent security service.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSP-1

Checks: DB-DG0110-Generic (Manual)
Review the services and processes active on the DBMS host system.

If the host system is acting as a Windows domain controller, this is a finding.

If the host system is supporting any other directory or security service that does not use the DBMS to store the directory information, this is a Finding.

Note: A local installation of Anti-virus or Firewall does not constitute a security service in this context.

Fixes: DB-DG0110-Generic (Manual)

Either move the DBMS installation to a dedicated host system or move the directory or security services to another host system.

A dedicated host system in this case refers to an instance of the operating system at a minimum.

The operating system may reside on a virtual host machine if supported by the DBMS vendor.

Vulnerability Key: V0015147

STIG ID: DG0111

Release Number: 7

Status: Active

Short Name: DBMS dedicated software directories

Long Name: The DBMS data files, transaction logs and audit files should be stored in dedicated directories or disk partitions separate from software or other application files.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0111-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Protection of DBMS data, transaction and audit data files stored by the host operating system is dependent on OS controls. When different applications share the same database process, resource contention and differing security controls may be required to isolate and protect one application's data and audit logs from another. DBMS software libraries and configuration files also require differing access control lists.

Default Finding Details: The DBMS data files, transaction logs or audit files are not stored in dedicated directories or disk partitions separate from software or other application files.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPA-1

Checks: DB-DG0111-Generic (Manual)

Review the disk/directory specification where database data, transaction log and audit files are stored.

If DBMS data, transaction or audit data files are stored in the same directory, this is a Finding.

If separation of data, transaction and audit data is not supported by the DBMS, this check is Not a Finding.

If stored separately and access permissions for each directory is the same, this is a Finding.

Fixes:

DB-DG0111-Generic (Manual)

Specify dedicated directories for storage of database data, transaction and audit files.

Configure DBMS default file storage locations to use dedicated directories where supported by the DBMS.

Ensure access permissions for each directory is customized to allow access only by authorized users and processes.

Vulnerability Key: V0015623

STIG ID: DG0112

Release Number: 7

Status: Active

Short Name: DBMS system data file protection

Long Name: DBMS system data files should be stored in dedicated disk directories.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0112-Generic

Severity: Category II

Severity

Override

Guidance:

Vulnerability Discussion: DBMS system data files have different access control requirements than application data and log files. Granting access to system data files beyond those required for system operations could lead to a compromise of the DBMS integrity or disclosure of sensitive data.

Default

Finding

Details:

DBMS system data files are not stored in dedicated disk directories.

Documentable: No

Documentable

Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18

Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPA-1

Checks: DB-DG0112-Generic (Manual)
Review the file and disk storage specification for the database data files.

If files other than those listed for the system tables are located in the same disk directory as the system database files, this is a Finding.

Fixes: DB-DG0112-Generic (Manual)
Configure dedicated disk directories to store DBMS data files that contain the DBMS system tables where supported by the DBMS.

Locate the DBMS system table data files on a dedicated disk partition where supported by the DBMS.

Vulnerability Key: V0015624

STIG ID: DG0113

Release Number: 4

Status: Active

Short Name: DBMS dedicated data files

Long Name: DBMS data files should be dedicated to support individual applications.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0113-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: DBMS data files may contain database objects supporting different applications. Shared resources and access to storage locations may lead to one application being vulnerable to the exploit or resource needs of the other. Dedicating data files to each application provides a means to separate by privilege assignment and resource quotas and protect one application from security issues of another.

Default Finding Details: DBMS data files are not dedicated to support individual applications.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCPA-1

Checks: DB-DG0113-Generic (Manual)

Review application database tables and their database file assignments.

If application database tables from unrelated applications are stored in the same database data files, this is a Finding.

Fixes: DB-DG0113-Generic (Manual)

Relocate application database tables to distinct database data files where supported by the DBMS.

Vulnerability Key: V0015119

STIG ID: DG0114

Release Number: 6

Status: Active

Short Name: Critical DBMS Files Fault Protection

Long Name: DBMS files critical for DBMS recovery should be stored on RAID or other high-availability storage devices.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0114-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: DBMS recovery can be adversely affected by hardware storage failure. Impediments to DBMS recovery can have a significant impact on operations.

Default Finding Details: DBMS files critical for DBMS recovery are not stored on RAID or other high-availability storage devices.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation COBR-1

Checks: DB-DG0114-Generic (Interview)
Interview the System Administrator to determine if the DBMS supports and employs DBMS high-availability redundancy such as DBMS or OS clustering.

If so, this check is Not a Finding.

Review the file and disk storage specification for the DBMS. Review the host disk system configuration for the host system.

If the disk is not part of a RAID or other disk fault-tolerant storage device, this is a Finding.

Fixes: DB-DG0114-Generic (Manual)
Place DBMS critical files including data, transaction and audit log files on fault-tolerant storage devices or employ DBMS or OS clustering where supported by the DBMS.

Vulnerability Key: V0015625

STIG ID: DG0115

Release Number: 4

Status: Active

Short Name: DBMS trusted recovery

Long Name: Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0115-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: A DBMS may be vulnerable to use of compromised data or other critical files during recovery. Use of compromised files could introduce maliciously altered application code, relaxed security settings or loss of data integrity. Where available, DBMS mechanisms to ensure use of only trusted files can help protect the database from this type of compromise during DBMS recovery.

Default Finding: Recovery procedures or technical system features do not exist to ensure that recovery is done in a secure and verifiable manner.

Details:**Documentable:** No**Documentable****Explanation:****Responsibility:** Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation COTR-1
 Database Security Technical Implementation Guide 3.5.5

Checks: DB-DG0115-Generic (Manual)

Review DBMS recovery procedures and technical system features to determine if mechanisms exist and are in place to specify use of trusted files during DBMS recovery.

If recovery procedures do not exist or are not sufficient to ensure recovery is done in a secure and verifiable manner, this is a Finding.

If system features exist and are not employed or not employed sufficiently, this is a Finding.

If circumstances that can inhibit a trusted recovery are not documented and appropriate mitigating procedures have not been put in place, this is a Finding.

Fixes: DB-DG0115-Generic (Manual)

Develop, document and implement DBMS recovery procedures and employ technical system features where supported by the DBMS to specify trusted files during DBMS recovery.

Ensure circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.

Vulnerability Key: V0015626**STIG ID:** DG0116**Release Number:** 4**Status:** Active**Short Name:** DBMS privileged role assignments**Long Name:** Database privileged role assignments should be restricted to IAO-authorized DBMS accounts.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0116-Generic

Severity: Category II

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** Roles assigned privileges to perform DDL and/or system configuration actions in the database can lead to compromise of any data in the database as well as operation of the DBMS itself. Restrict assignment of privileged roles to authorized personnel and database accounts to help prevent unauthorized activity.

**Default
Finding
Details:**

Database privileged role assignments are not restricted to IAO-authorized DBMS accounts.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks:

DB-DG0116-Generic (Manual)

Review a list of privileged role assignments in the database.

Roles having privileges other than SELECT, UPDATE, DELETE, and EXECUTE constitute privileges of interest.

Compare the listed assignments against the evidence of IAO authorization for the role assignments.

If any roles contain members that are not documented as authorized by the IAO, this is a Finding.

Fixes:

DB-DG0116-Generic (Manual)

Document IAO-authorized privileged role assignments in the System Security Plan.

Remove assignments where not authorized.

Vulnerability Key: V0015127

STIG ID: DG0118

Release Number: 8

Status: Active

Short Name: IAM review of change in DBA assignments

Long Name: The IAM should review changes to DBA role assignments.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality	I - Mission Critical	II - Mission Support	III - Administrative

Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0118-Generic

Severity: Category II

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** Unauthorized assignment of DBA privileges can lead to a compromise of DBMS integrity. Providing oversight to the authorization and assignment of privileges provides the separation of duty to support sufficient oversight.

**Default
Finding
Details:** The IAM is not reviewing changes to DBA role assignments.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Manager

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECPA-1

Checks: DB-DG0118-Generic (Manual)
Review the policy, procedures and implementation evidence for monitoring changes to DBA role assignments and procedures for notifying the IAM of the changes for review.

If policy, procedures and implementation evidence do not exist, this is a Finding.

Fixes: DB-DG0118-Generic (Manual)
Develop, document and implement policy and procedures to monitor changes to DBA role assignments.

Develop, document and implement policy and procedures to notify the IAM of changes to DBA role assignments.

Include methods in the procedures that provide evidence of monitoring and notification.

Vulnerability Key: V0015631

STIG ID: DG0123

Release Number: 4

Status: Active

Short Name: DBMS Administrative data access

Long Name: Access to DBMS system tables and other configuration or metadata should be restricted to DBAs.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0123-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Administrative data includes DBMS metadata and other configuration and management data. Unauthorized access to this data could result in unauthorized changes to database objects, access controls, or DBMS configuration.

Default Finding Details: Access to DBMS system tables and other configuration or metadata is not restricted to DBAs.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAN-1

Checks: DB-DG0123-Generic (Manual)
Review access controls on system tables.

Review access to configuration data stored in the database.

If any users not assigned DBA privileges are assigned access to the underlying tables, this is a Finding.

Fixes: DB-DG0123-Generic (Manual)
Revoke access to system tables to non-DBA users.

Where use of system data is required by non-DBA users, provide controlled access for authorized functions via views, procedures, or other use of controlled objects.

Vulnerability Key: V0015632

STIG ID: DG0124

Release Number: 4

Status: Active

Short Name: DBA account use

Long Name: Use of DBA accounts should be restricted to administrative activities.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--------------------------------------------------------------------------------------------------------------------	------------------------------

☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0124-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Use of privileged accounts for non-administrative purposes puts data at risk of unintended or unauthorized loss, modification or exposure. In particular, DBA accounts if used for non-administration application development or application maintenance can lead to miss-assignment of privileges where privileges are inherited by object owners. It may also lead to loss or compromise of application data where the elevated privileges bypass controls designed in and provided by applications.

Default Finding Details:

Use of DBA accounts is not restricted to administrative activities.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLP-1

Checks:

DB-DG0124-Generic (Manual)

Review objects owned by custom DBA user accounts.

If any objects owned by DBA accounts are accessed by non-DBA users either directly or indirectly by other applications, this is a Finding.

Review documentation or instructions provided to DBAs to communicate proper and improper use of DBA accounts.

If such documentation does not exist or if DBAs do not indicate an understanding of this requirement, this is a Finding.

Fixes:

DB-DG0124-Generic (Manual)

Develop, document and implement policy and procedures for outlining the proper and improper use of DBA accounts.

The documentation should clearly state that DBA accounts are used to administer and maintain the database only.

DBA accounts are not to be used to create or alter application objects.

Application maintenance should always be performed by the application object owner or application administrator accounts.

Request acknowledgement of receipt of these restrictions by all users granted DBA

responsibilities.

Vulnerability Key: V0015633

STIG ID: DG0126

Release Number: 4

Status: Active

Short Name: DBMS account password reuse

Long Name: Password reuse should be prevented where supported by the DBMS.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0126-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Password reuse restrictions protect against bypass of password expiration requirements and help protect accounts from password guessing attempts. The DoDI 8500.2 specifies preventing password reuse to the extent system capabilities permit.

Default Finding Details: Password reuse is not prevented where supported by the DBMS.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2
 Database Security Technical Implementation Guide 3.2.2.2

Checks: DB-DG0126-Generic (Manual)

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

Review DBMS account password reuse restrictions.

If the DBMS is not configured to prevent password reuse, this is a Finding.

If the DBMS uses Host Authentication, confirm that the host is configured to prevent password

reuse. If it is not, this is a Finding.

Fixes:

DB-DG0126-Generic (Manual)

Configure the DBMS to prevent password reuse where supported by the DBMS.

Where Host Authentication is used, configure the OS to prevent password reuse.

Consider configuring the DBMS to use alternate authentication methods other than password authentication where supported by the DBMS.

Vulnerability Key: V0015635

STIG ID: DG0128

Release Number: 4

Status: Active

Short Name: DBMS default passwords

Long Name: DBMS default accounts should be assigned custom passwords.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0128-Generic

Severity: Category I

Severity Override Guidance: If identified accounts show an account status of LOCKED and password is set to EXPIRED this is a Finding, but downgrade the severity Category Code to II.

Vulnerability Discussion: DBMS default passwords provide a commonly known and exploited means for unauthorized access to database installations.

Default Finding Details: DBMS default accounts have not been assigned custom passwords.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0128-Generic (Manual)

This check is applicable regardless of database enablement of password authentication or other

means such as account disablement or locking to protect default accounts.

The only exception is for accounts using host authentication.

Review the list of DBMS user accounts.

Confirm or verify all accounts created by the DBMS installation.

Obtain default password information for the default accounts in vendor documentation, through Internet searches, or other means if possible.

Test accounts for passwords set to default values.

If any are found, this is a Finding.

Fixes:

DB-DG0128-Generic (Manual)

Set passwords for DBMS accounts to non-default values. Where necessary, unlock or enable accounts to set the password and then return the account to disabled or locked status.

Vulnerability Key: V0015636

STIG ID: DG0129

Release Number: 4

Status: Active

Short Name: DBMS passwords in transit

Long Name: Passwords should be encrypted when transmitted across the network.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0129-Generic

Severity: Category I

Severity Override Guidance:

Vulnerability Discussion: DBMS passwords sent in clear text format across the network are vulnerable to discovery by unauthorized users. Disclosure of passwords may easily lead to unauthorized access to the database.

Default Finding Details: Passwords are not encrypted when transmitted across the network.

Documentable: No

Documentable

Explanation:**Responsibility:** Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2
 Database Security Technical Implementation Guide 3.2.2.1

Checks: DB-DG0129-Generic (Manual)

Review configuration options for encrypting passwords during login events across the network.

If passwords are not encrypted, this is a Finding.

If determined that passwords are passed unencrypted at any point along the transmission path between the source and destination, this is a Finding.

Fixes: DB-DG0129-Generic (Manual)

Configure encryption for transmission of passwords across the network.

If the database does not provide encryption for login events natively, employ encryption at the OS or network level.

Ensure passwords remain encrypted from source to destination.

Vulnerability Key: V0015637**STIG ID:** DG0130**Release Number:** 5**Status:** Active**Short Name:** DBMS passwords in batch and applic. source code**Long Name:** DBMS passwords should not be stored in compiled, encoded or encrypted batch jobs or compiled, encoded or encrypted application source code.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0130-Generic**Severity:** Category II**Severity Override****Guidance:**

Vulnerability Discussion: The storage of passwords in application source or batch job code that is compiled, encoded or encrypted prevents compliance with password expiration and other management requirements as

well as provides another means for potential discovery.

Default Finding Details:

DBMS passwords are stored in compiled, encoded or encrypted batch jobs or compiled, encoded or encrypted application source code.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0130-Generic (Interview)

Ask the DBA to review application source code that is required by Check DG0091 to be encoded or encrypted for database accounts used by applications or batch jobs to access the database.

Ask the DBA to review source batch job code prior to compiling, encoding or encrypting for database accounts used by applications or the batch jobs themselves to access the database.

Ask the DBA and/or IAO to determine if the compiled, encoded or encrypted application source code or batch jobs contain passwords used for authentication to the database.

If none of the identified compiled, encoded or encrypted application source code or batch job code contain passwords used for authentication, this check is Not a Finding.

If any of the identified compiled, encoded or encrypted application source code or batch job code do contain passwords used for authentication to the database, this is a Finding.

NOTE: This check only applies to application source code or batch job code that is compiled, encoded or encrypted in a production environment. Application source code or batch job code that is not compiled, encoded or encrypted would fall under Check DG0067 for determination of compliance.

Fixes: DB-DG0130-Generic (Manual)

Design DBMS application code and batch job code that is compiled, encoded or encrypted to NOT contain passwords.

Consider alternatives to using password authentication for compiled, encoded or encrypted batch jobs and DBMS application code.

Vulnerability Key: V0015638

STIG ID: DG0131

Release Number: 4

Status: Active

Short Name: DBMS default account names

Long Name: DBMS default account names should be changed.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0131-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Well-known DBMS account names are targeted most frequently by attackers and are thus more prone to providing unauthorized access to the database.

Default Finding Details: DBMS default account names have not been changed.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation IAIA-1, IAIA-2

Checks: DB-DG0131-Generic (Manual)

If the DBMS does not support changes to default account names, this check is Not Applicable only for those accounts that cannot be altered.

Review the list of default account names provided by the DBMS.

The list may be provided in vendor documentation or obtained using Internet resources.

If default account names exist, this is a Finding.

Fixes: DB-DG0131-Generic (Manual)

Where supported by the DBMS, modify default DBMS accounts to use custom account names.

To maintain consistency with similar DBMS products; develop, document and implement site policy and procedure to regulate changes to default account names.

Vulnerability Key: V0015640

STIG ID: DG0134

Release Number: 4

Status: Active

Short Name: DBMS concurrent connections

Long Name: Concurrent connections to the DBMS should be limited and controlled.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--------------------------------------------------------------------------------------------------------------------	--------------------------

☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0134-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Unlimited concurrent connections to the DBMS could allow a successful Denial of Service (DoS) attack by exhausting connection resources.

Default Finding Details: Concurrent connections to the DBMS are not limited or controlled.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLO-1, ECLO-2

Checks: DB-DG0134-Generic (Manual)
If the DBMS does not provide concurrent connection controls, this check is Not a Finding.

If limiting concurrent connections is not recommended by the DBMS vendor or implementation adversely affects supported GOTS or COTS applications, this check is Not a Finding.

Review the concurrent connection control settings. If controls are not set or do not match the setting specified in the System Security Plan, this is a Finding.

Fixes: DB-DG0134-Generic (Manual)
Determine a reasonable limitation for concurrent connection requests to support operation of the application.

Configure the DBMS to limit concurrent connections to the determined number.

Document the limit in the System Security Plan.

Vulnerability Key: V0015643

STIG ID: DG0140

Release Number: 7

Status: Active

Short Name: DBMS security data access

Long Name: Access to DBMS security should be audited.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0140-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: DBMS security data is useful to malicious users to perpetrate activities that compromise DBMS operations or data integrity. Auditing of access to this data supports forensic and accountability investigations.

Default Finding Details:

Access to DBMS security data is not audited.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-1, ECAR-2, ECAR-3

Checks: DB-DG0140-Generic (Manual)

Determine locations of DBMS audit, configuration, credential and other security data. Review audit settings for these files or data objects.

If the security data is not audited for access, consider the operational impact and appropriateness for access that is not audited.

If the risk for incomplete auditing of the security files is reasonable and documented in the System Security Plan, do not include this as a Finding.

Fixes: DB-DG0140-Generic (Manual)

Determine all locations for storage of DBMS security and configuration data.

Enable auditing for access to any security data where supported by the DBMS.

If audit for access results in an unacceptable adverse impact on application operation, scale back the audit to a reasonable and acceptable level.

Document any incomplete audit with acceptance of the risk of incomplete audit in the System Security Plan.

Vulnerability Key: V0015644

STIG ID: DG0141

Release Number: 4

Status: Active

Short Name: DBMS access control bypass

Long Name: Attempts to bypass access controls should be audited.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0141-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Detection of suspicious activity including access attempts and successful access from unexpected places, during unexpected times, or other unusual indicators can support decisions to apply countermeasures to deter an attack. Without detection, malicious activity may proceed without impedance.

Default

Finding Details: Attempts to bypass access controls is not audited.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-2, ECAR-3

Checks: DB-DG0141-Generic (Manual)

Review any audit settings for the following activities. If any of these activities are covered in other checks, do not include in this check:

- unsuccessful logon attempts
- account locking events
- account disabling from a specific source location
- failed database object attempts or attempts to access objects that do not exist
- other activities that may produce unexpected failures or trigger DBMS lockdown actions

If any of the above events as applicable to the DBMS are not audited, this is a Finding.

Fixes:

DB-DG0141-Generic (Manual)

Configure auditing to capture the events listed below where available in the DBMS:

- unsuccessful logon attempts
- account locking events
- account disabling from a specific source location
- failed database object attempts or attempts to access objects that do not exist
- other activities that may produce unexpected failures or trigger DBMS lockdown actions

If audit for these events results in an unacceptable adverse impact on application operation, scale back the audit to a reasonable and acceptable level.

Document any incomplete audit with acceptance of the risk of incomplete audit in the System Security Plan.

Vulnerability Key: V0015645

STIG ID: DG0142

Release Number: 4

Status: Active

Short Name: DBMS Privileged action audit

Long Name: Changes to configuration options should be audited.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0142-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Changes to security labels or markings may indicate possible tampering to facilitate unauthorized access or malicious activity.

Default Finding Details: Changes to configuration options are not audited.

Documentable: No

Documentable

Explanation:

Responsibility: Database Administrator

References:

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)

Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-3

Checks: DB-DG0142-Generic (Manual)
 If the DBMS does not support the use of security labels or sensitivity markings, this check is Not Applicable.

Review audit settings for changes to security labels or sensitivity markings.

If changes are not audited, this is a Finding.

Fixes: DB-DG0142-Generic (Manual)
 Configure and enable auditing of changes to security labels and sensitivity markings where supported by the DBMS.

Vulnerability Key: V0015646

STIG ID: DG0145

Release Number: 4

Status: Active

Short Name: DBMS audit record content

Long Name: Audit records should contain required information.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0145-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Complete forensically valuable data may be unavailable or accountability may be jeopardized when audit records do not contain sufficient information.

Default Finding Details: Audit records do not contain required information.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18

Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-1

Checks:

DB-DG0145-1-Generic (Manual)

Review samples of the DBMS audit logs.

Compare to the required elements listed below:

- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.

If the elements listed above are not included in the audit logs at at minimum, this is a Finding.

Fixes:

DB-DG0145-1-Generic (Manual)

Configure audit settings to include the following list of elements in the audit logs at a minimum:

- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition:

Generic Database Installation (Target: Generic Database Installation)

Policy:

All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID:

DG0145-Generic

Severity:

Category II

Severity Override**Guidance:****Vulnerability**

Complete forensically valuable data may be unavailable or accountability may be jeopardized when audit records do not contain sufficient information.

Discussion:**Default Finding Details:**

Audit records do not contain required information.

Documentable:

No

Documentable Explanation:**Responsibility:**

Database Administrator

References:

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-2

Checks:

DB-DG0145-2-Generic (Manual)

Review samples of the DBMS audit logs.

Compare to the required elements listed below:

- 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.

If the elements listed above are not included in the audit logs at at minimum, this is a Finding.

Fixes:

DB-DG0145-2-Generic (Manual)

Configure audit settings to include the following list of elements in the audit logs at a minimum:

- 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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0145-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Complete forensically valuable data may be unavailable or accountability may be jeopardized when audit records do not contain sufficient information.

Default Finding Details: Audit records do not contain required information.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-3

Checks: DB-DG0145-3-Generic (Manual)
Review samples of the DBMS audit logs.

Compare to the required elements listed below:

- 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.
- Data required to audit the possible use of covert channel mechanisms.
- Privileged activities and other system-level access.
- Starting and ending time for access to the system.
- Security relevant actions associated with periods processing or the changing of security labels or categories of information.

If the elements listed above are not included in the audit logs at at minimum, this is a Finding.

Fixes: DB-DG0145-3-Generic (Manual)
Configure audit settings to include the following list of elements in the audit logs at a minimum:

- 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.
- Data required to audit the possible use of covert channel mechanisms.
- Privileged activities and other system-level access.
- Starting and ending time for access to the system.
- Security relevant actions associated with periods processing or the changing of security labels or categories of information.

Vulnerability Key: V0015647

STIG ID: DG0146

Release Number: 4

Status: Active

Short Name: DBMS connection block audit

Long Name: Audit records should include the reason for blacklisting or disabling DBMS connections or accounts.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality	I - Mission Critical	II - Mission Support	III - Administrative

Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0146-Generic

Severity: Category II

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** Records of any disabling or locking of account actions taken by the DBMS can contain information valuable to decisions to employ additional responsive actions.

**Default
Finding
Details:** Audit records do not include the reason for blacklisting or disabling DBMS connections or accounts.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAR-2, ECAR-3

Checks: DB-DG0146-Generic (Manual)
Review audit settings for disabling or locking account events based on event failures.

If the settings are not configured to include the cause of the lock or disabling, this is a Finding.

Fixes: DB-DG0146-Generic (Manual)
Develop, document and implement audit settings that will collect and store the cause of any DBMS account or connection lock or disabling actions taken by the DBMS.

Vulnerability Key: V0015648

STIG ID: DG0151

Release Number: 4

Status: Active

Short Name: DBMS random port use

Long Name: Access to the DBMS should be restricted to static, default network ports.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
STIG ID:	DG0151-Generic			
Severity:	Category II			
Severity Override Guidance:				
Vulnerability Discussion:	Use of static, default ports helps management of enterprise network device security controls. Use of non-default ports makes tracking and protection of published vulnerabilities to services and protocols more difficult to track and block and may result in the exposure of the database to unintended network segments and users.			
Default Finding Details:	Access to the DBMS is not restricted to static, default network ports.			
Documentable:	No			
Documentable Explanation:				
Responsibility:	Database Administrator			
References:	Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8) Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCP-1			
Checks:	DB-DG0151-Generic (Manual) If remote access to the DBMS via a database listener, ODBC or direct TCP/UDP connection is not enabled, this check is Not a Finding. Review DBMS network listener, network and ODBC connections and the configuration options that control remote network access to the DBMS. If any indicate the use of dynamic ports, this is a Finding.			
Fixes:	DB-DG0151-Generic (Manual) Configure the DBMS network listener, network and ODBC connections to use static, default ports. Refer to vendor documentation for a list of default ports.			

Vulnerability Key: V0015148

STIG ID: DG0152

Release Number: 6

Status: Active

Short Name: DBMS network port, protocol and services (PPS) use

Long Name: DBMS network communications should comply with PPS usage restrictions.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0152-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Use of default ports is required in DoD networks to support network security device management.

Default Finding Details: DBMS network communications do not comply with PPS usage restrictions.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCP-1

Checks: DB-DG0152-Generic (Manual)
Review the standard or registered ports for the DBMS.

Search the DBMS vendor documentation or:

<http://www.iana.org/assignments/port-numbers>

to determine default ports.

If any port value is set to a different port than the registered or standard port number, verify that network communications to or from the DBMS do not cross network or enclave boundaries as defined in the PPS CAL:

<http://iase.disa.mil/ports/index.html>

If any do, this is a Finding.

Fixes: DB-DG0152-Generic (Manual)
Configure DBMS network communications to use standard ports as defined by the DBMS vendor or at:

<http://www.iana.org/assignments/port-numbers>

Ensure network access outside the Enclave is permitted in the PPS CAL:

<http://iase.disa.mil/ports/index.html>

Vulnerability Key: V0015149

STIG ID: DG0153

Release Number: 7

Status: Active

Short Name: DBMS DBA roles assignment approval

Long Name: DBA roles assignments should be assigned and authorized by the IAO.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0153-Generic

Severity: Category III

Severity Override

Guidance:

Vulnerability Discussion: The DBA role and associated privileges provide complete control over the DBMS operation and integrity. DBA role assignment without authorization could lead to the assignment of these privileges to untrusted and untrustworthy persons and complete compromise of DBMS integrity.

Default Finding Details:

DBA roles assignments are not assigned and authorized by the IAO.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSD-1

Checks: DB-DG0153-Generic (Manual)

Review the documented procedures for approval and granting of DBA privileges.

Review implementation evidence for the procedures.

If procedures do not exist or evidence that they are followed does not exist, this is a Finding.

Fixes: DB-DG0153-Generic (Manual)

Develop, document and implement procedures to ensure all DBA role assignments are authorized and assigned by the IAO.

Include methods that provide evidence of approval in the procedures.

Vulnerability Key: V0015150

STIG ID: DG0154

Release Number: 8

Status: Active
Short Name: DBMS System Security Plan
Long Name: The DBMS requires a System Security Plan containing all required information.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0154-Generic

Severity: Category III

Severity Override

Guidance:

Vulnerability Discussion: A System Security Plan identifies security control applicability and configuration for the DBMS. It also contains security control documentation requirements. Security controls applicable to the DBMS may not be documented, tracked or followed if not identified in the System Security Plan. Any omission of security control consideration could lead to an exploit of DBMS vulnerabilities.

Default Finding Details: The DBMS does not have a System Security Plan or the System Security Plan does not contain the required information.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSD-1

Checks: DB-DG0154-Generic (Interview)

Review the System Security Plan for the DBMS with the IAO.

Review coverage of the following in the System Security Plan:

1. Technical, administrative and procedural IA program and policies that govern the DBMS
2. Identification of all IA personnel (IAM, IAO, DBA, SA) assigned responsibility to the DBMS
3. Specific IA requirements and objectives (e.g., requirements for data handling or dissemination (to include identification of sensitive data stored in the database, database application user job functions/roles and privileges), system redundancy and backup, or emergency response)

If the System Security Plan does not exist, this is a Finding.

If the System Security Plan does not include the information listed above at a minimum, this is a Finding.

Fixes: DB-DG0154-Generic (Manual)

Develop, document and implement a System Security Plan for the DBMS or include IA

documentation related to the DBMS in the System Security Plan of the system that the DBMS supports.

A template for creating an SSP may be found on the DIACAP Knowledge Service:

<https://diacap.iaportal.navy.mil/>

Links:

DIACAP Resources -> DIACAP Reference Library -> Sample Documents -> ISP_Sample.doc (zipped)

or the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems. This document may be found at:

<http://csrc.nist.gov/publications/PubsSPs.html>

Include or note additional information in the System Security Plan where required in other DBMS checks.

Vulnerability Key: V0015649

STIG ID: DG0155

Release Number: 4

Status: Active

Short Name: DBMS System State Changes

Long Name: The DBMS should have configured all applicable settings to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0155-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The DBMS opens data files and reads configuration files at system startup, system shutdown and during abort recovery efforts. If the DBMS does not verify the trustworthiness of these files, it is vulnerable to malicious alterations of its configuration or unauthorized replacement of data.

Default Finding Details: The DBMS does not have configured all applicable settings to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator
Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSS-1, DCSS-2

Checks: DB-DG0155-Generic (Interview)

Ask the DBA and/or IAO to demonstrate that the DBMS system initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.

If the DBA and/or IAO has documented proof from the DBMS vendor demonstrating that the DBMS does not support this either natively or programmatically, this check is a Finding, but can be downgraded to a CAT 3 severity.

If the DBMS does support this either natively or programmatically and the configuration does not meet the requirements listed above, this is a Finding.

For all MAC 1, all MAC 2 and Classified MAC 3 systems where the DBMS supports the requirements, review documented procedures and evidence of periodic testing to ensure DBMS system state integrity.

If documented procedures do not exist or no evidence of implementation is provided, this is a Finding.

Fixes: DB-DG0155-Generic (Manual)

Configure DBMS system initialization, shutdown and aborts to ensure DBMS system remains in a secure state.

For applicable DBMS systems as listed in the check, periodically test configuration to ensure DBMS system state integrity.

Where DBMS system state integrity is not supported by the DBMS vendor, obtain and apply mitigation strategies to bring risk to a DAA-acceptable level.

Vulnerability Key: V0015650

STIG ID: DG0156

Release Number: 4

Status: Active

Short Name: DBMS IAO assignment

Long Name: The IAO for the DBMS should be assigned and authorized by the IAM.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC /

	I - Mission Critical	II - Mission Support	III - Administrative
--	-----------------------------	-----------------------------	-----------------------------

Confidentiality Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0156-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Database Management Systems whose security configuration is not overseen by authorized personnel are subject to vulnerable configurations. This provides a separation of duties for the administration of the DBMS where operational priorities may conflict with security requirements.

Default Finding Details: The IAO for the DBMS is not assigned or authorized by the IAM.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Manager

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCSD-1

Checks: DB-DG0156-Generic (Manual)
Review evidence of IAM assignment and authorization of IAO responsibilities for the DBMS.

If the IAO is not authorized by the IAM or evidence of the authorization does not exist, this is a Finding.

Fixes: DB-DG0156-Generic (Manual)
Develop, document and implement policy and procedures for assignment of IAO responsibilities for the DBMS.

Include methods to provide evidence of the assignment. This may be accomplished using email or other verifiable electronic means or by hardcopy.

Document the procedures for assignment and evidence in the System Security Plan.

Vulnerability Key: V0015651

STIG ID: DG0157

Release Number: 5

Status: Active

Short Name: DBMS remote administration

Long Name: Remote DBMS administration should be documented and authorized or disabled.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0157-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Remote administration may expose configuration and sensitive data to unauthorized viewing during transit across the network or allow unauthorized administrative access to the DBMS to remote users.

Default Finding Details:

Remote DBMS administration is not documented, not authorized or is not disabled.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation EBRP-1

Checks: DB-DG0157-Generic (Manual)

If the DBMS does not support remote DBMS administration, this check is Not Applicable.

If the DBMS supports remote DBMS administration, Review the System Security Plan for authorization, assignments and usage procedures.

If remote administration of the DBMS is not documented or poorly documented, this is a Finding.

If remote administration of the DBMS is not authorized and not disabled, this is a Finding.

Fixes: DB-DG0157-Generic (Manual)

Disable remote administration of the DBMS where not required.

Where remote administration of the DBMS is required, develop, document and implement policy and procedures on its use.

Assign remote administration privileges to IAO-authorized personnel only.

Document in the System Security Plan.

Vulnerability Key: V0015652

STIG ID: DG0158

Release Number: 4

Status: Active

Short Name: DBMS remote administration audit

Long Name: DBMS remote administration should be audited.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0158-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: When remote administration is available, the vulnerability to attack for administrative access is increased. An audit of remote administrative access provides additional means to discover suspicious activity and to provide accountability for administrative actions completed by remote users.

Default Finding Details: DBMS remote administration is not audited.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation EBRP-1

Checks: DB-DG0158-Generic (Manual)

If the DBMS does not provide auditing of remote administrative actions, this check is Not a Finding.

Review settings for actions taken during remote administration sessions.

If auditing of remote administration sessions and actions is not enabled, this is a Finding.

If audit logs do not include all actions taken by database administrators during remote sessions, this is a Finding.

Fixes: DB-DG0158-Generic (Manual)

Develop, document and implement policy and procedures for remote administration auditing.

Configure the DBMS to provide an audit trail for remote administrative sessions.

Include all actions taken by database administrators during remote sessions.

Actions should be tied to a specific user.

Vulnerability Key: V0015118

STIG ID: DG0159

Release Number: 8

Status: Active

Short Name: Review of DBMS remote administrative access

Long Name: Remote administrative access to the database should be monitored by the IAO or IAM.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0159-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: Remote administrative access to systems provides a path for access to and exploit of DBA privileges. Where the risk has been accepted to allow remote administrative access, it is imperative to enstate increased monitoring of this access to detect any abuse or compromise.

Default Finding Details:

Remote administrative access to the database is not monitored by the IAO or IAM.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer
Information Assurance Manager

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation EBRP-1

Checks: DB-DG0159-Generic (Interview)

If remote administrative access to the database is disabled, this check is Not a Finding.

Review policy, procedures and implementation evidence of monitoring of remote administrative access to the database with the IAO or IAM.

If policy and procedures for monitoring remote administrative access do not exist or not implemented, this is a Finding.

Fixes: DB-DG0159-Generic (Manual)

Develop, document and implement policy and procedures to monitor remote DBA access to the DBMS.

The automated generation of a log report with automatic dissemination to the IAO and/or IAM may be used.

Require and store an acknowledgement of receipt and confirmation of review for the log report.

Vulnerability Key: V0015653

STIG ID: DG0160

Release Number: 4

Status: Active

Short Name: DBMS failed login limit

Long Name: The DBMS should limit failed logins within a specified time period.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0160-Generic

Severity: Category III

Severity Override Guidance:

Vulnerability Discussion: Unrestricted failed login attempts allow brute force attacks on DBMS user accounts. More recent brute force attacks make attempts over long periods of time to circumvent intrusion detection systems and system account lockouts based entirely on the number of failed logins that are typically reset after a successful login.

Default Finding Details: The DBMS does not limit failed logins within a specified time period.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECLO-1, ECLO-2

Checks: DB-DG0160-Generic (Manual)
 If the DBMS does not provide a means to restrict the number of failed logins within a specified time period, this check is Not Applicable.

Compare the DBMS configuration for the number of failed logins allowed within the allowed time

period against that documented in the System Security Plan.

If the settings do not match the settings as specified in the System Security Plan, this is a Finding.

Fixes:

DB-DG0160-Generic (Manual)

Set the failed login limit and time period in accordance with the System Security Plan where supported by the DBMS.

Vulnerability Key: V0015103

STIG ID: DG0161

Release Number: 8

Status: Active

Short Name: DBMS Audit Tool

Long Name: An automated tool that monitors audit data and immediately reports suspicious activity should be employed for the DBMS.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0161-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Audit logs can capture information on suspicious events. Without an automated monitoring and alerting tool, malicious activity may go undetected and without response until compromise of the database or data is severe.

Default Finding Details: An automated tool that monitors audit data and immediately reports suspicious activity is not employed for the DBMS.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECAT-2

Checks: DB-DG0161-Generic (Interview)

Review evidence or operation of an automated, continuous on-line monitoring and audit trail

creation capability for the DBMS 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 system if serious IA violations are detected.

If the requirements listed above are not fully met, this is a Finding.

Fixes:

DB-DG0161-Generic (Manual)

Develop or procure, document and implement an automated, continuous on-line monitoring and audit trail creation capability for the DBMS 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 system if serious IA violations are detected.

Vulnerability Key: V0015104

STIG ID: DG0167

Release Number: 7

Status: Active

Short Name: Encryption of DBMS sensitive data in transit

Long Name: Sensitive data served by the DBMS should be protected by encryption when transmitted across the network.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0167-Generic

Severity: Category I

Severity

Override

Guidance:

Vulnerability Discussion: Sensitive data served by the DBMS and transmitted across the network in clear text is vulnerable to unauthorized capture and review.

Default Finding Details: Sensitive data served by the DBMS is not protected by encryption when transmitted across the network.

Documentable: No

Documentable

Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
 Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
 Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECCT-1, ECCT-2

Checks: DB-DG0167-Generic (Interview)

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

If encryption requirements are listed and specify configuration at the host system or network device level, review evidence that the configuration meets the specification with the DBA.

It may be necessary to review network device configuration evidence or host communications configuration evidence with a Network and/or System Administrator.

If the evidence review does not meet the requirement or specification as listed in the System Security Plan, this is a Finding.

Fixes: DB-DG0167-Generic (Manual)

Configure encryption of sensitive data served by the DBMS in accordance with the specifications provided in the System Security Plan and AIS Functional Architecture documentation.

Document acceptance of risk by the Information Owner where sensitive or classified data is not encrypted.

Have the IAO document assurance that the unencrypted sensitive or classified information is otherwise inaccessible to those who do not have Need-to-Know access to the data.

Vulnerability Key: V0015655

STIG ID: DG0170

Release Number: 4

Status: Active

Short Name: DBMS transaction journaling

Long Name: DBMS transaction journaling should be enabled.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0170-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability The maintenance of data integrity involves preservation and control of not only the data contents,

Discussion: but the relationships between two or more related data items and the actions taken on one that may affect others. A DBMS provides data integrity that may be affected by incomplete or interrupted transactions by means of logging transaction events. This allows the database to recover data content to a point where the data content and its relationships are known to be intact. This data integrity is maintained when the data is undergoing a change or update event. Most DBMS's enable transaction rollback or recovery by default and as an automatic feature of database recovery.

Default Finding Details: DBMS transaction journaling has not been enabled.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECDC-1

Checks: DB-DG0170-Generic (Manual)
Review DBMS settings that enable or disable transaction journaling.

If no configuration settings are available to enable or disable transaction journaling, this check is Not Applicable.

If settings are available and transaction journaling is disabled, this is a Finding.

Fixes: DB-DG0170-Generic (Manual)
Enable transaction journaling for the database where supported by the DBMS.

Vulnerability Key: V0015656

STIG ID: DG0171

Release Number: 4

Status: Active

Short Name: DBMS interconnections

Long Name: The DBMS should not have a connection defined to access or be accessed by a DBMS at a different classification level.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0171-Generic

Severity: Category II

**Severity
Override
Guidance:**

**Vulnerability
Discussion:** Applications that access databases and databases connecting to remote databases that differ in their assigned classification levels may expose sensitive data to unauthorized clients. Any interconnections between databases or applications and databases differing in classification levels are required to comply with interface control rules.

**Default
Finding
Details:** The DBMS has a connection defined to access or be accessed by a DBMS at a different classification level.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECIC-1

Checks: DB-DG0171-Generic (Manual)
Review database links or other connections defined for the database to access or be accessed by remote databases or other applications as defined in the AIS Functional Architecture documentation or the System Security Plan.

If any interconnections show differences in the DBMS and remote system classification levels, this is a Finding.

Fixes: DB-DG0171-Generic (Manual)
Disassociate or remove connection definitions to remote systems of differing classification levels.

Vulnerability Key: V0015116

STIG ID: DG0175

Release Number: 8

Status: Active

Short Name: DBMS host and component STIG compliancy

Long Name: The DBMS host platform and other dependent applications should be configured in compliance with applicable STIG requirements.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0175-Generic

Severity: Category II

**Severity
Override**

Guidance:

**Vulnerability
Discussion:** The security of the data stored in the DBMS is also vulnerable to attacks against the host platform, calling applications, and other application or optional components.

**Default
Finding
Details:** The DBMS host platform and other dependent applications are not configured in compliance with applicable STIG requirements.

Documentable: No

**Documentable
Explanation:**

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECSC-1

Checks: DB-DG0175-Generic (Interview)

Review evidence of security hardening and auditing of the DBMS host platform with the IAO.

If the DBMS host platform has not been hardened and received a security audit, this is a Finding.

Review evidence of security hardening and auditing for all application(s) that store data in the database and all other separately configured components that access the database including web servers, application servers, report servers, etc.

If any have not been hardened and received a security audit, this is a Finding.

Review evidence of security hardening and auditing for all application(s) installed on the local DBMS host where security hardening and auditing guidance exists.

If any have not been hardened and received a security audit, this is a Finding.

Fixes: DB-DG0175-Generic (Manual)

Configure all related application components and the DBMS host platform in accordance with applicable DoD STIG guidance.

Regularly audit the security configuration of related applications and the host platform to confirm continued compliance with security requirements.

Vulnerability Key: V0015117

STIG ID: DG0176

Release Number: 7

Status: Active

Short Name: DBMS audit log backups

Long Name: The DBMS audit logs should be included in backup operations.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0176-Generic

Severity: Category II

Severity Override

Guidance:

Vulnerability Discussion: DBMS audit logs are essential to the investigation and prosecution of unauthorized access to the DBMS data. Unless audit logs are available for review, the extent of data compromise may not be determined and the vulnerability exploited may not be discovered. Undiscovered vulnerabilities could lead to additional or prolonged compromise of the data.

Default Finding Details:

The DBMS audit logs are not included in backup operations.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECTB-1

Checks: DB-DG0176-Generic (Manual)

Review the DBMS locations for DBMS audit log files including both DBMS startup and shutdown as well as other DBMS-generated event log files.

Review the location of audit trail data stored externally to the DBMS.

Review backup procedures and/or reports to verify evidence of inclusion of DBMS log files in backup procedures.

If evidence of inclusion of audit, error, or any other DBMS-related log files in regular DBMS or host backups does not exist, this is a Finding.

Fixes: DB-DG0176-Generic (Manual)

Configure and ensure DBMS audit trace files, DBMS process and other error log files are included in regular backups.

Vulnerability Key: V0015658

STIG ID: DG0179

Release Number: 8

Status: Active

Short Name: DBMS warning banner

Long Name: The DBMS warning banner should meet DoD policy requirements.

<input type="checkbox"/> Open	Comments:
-------------------------------	-----------

☐ Not a Finding
☐ Not Applicable
☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0179-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Without sufficient warning of monitoring and access restrictions of a system, legal prosecution to assign responsibility for unauthorized or malicious access may not succeed. A warning message provides legal support for such prosecution. Access to the DBMS or the applications used to access the DBMS require this warning to help assign responsibility for database activities.

Default Finding Details: The DBMS warning banner does not meet DoD policy requirements.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECWM-1

Checks: DB-DG0179-Generic (Manual)

A warning banner displayed as a function of an Operating System or application login for applications that use the database makes this check Not Applicable.

View the warning banner. If it does not contain the following text as written below, this is a Finding:

[A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine

monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

[B. For Blackberries and other PDAs/PEDs with severe character limitations:]

I've read & consent to terms in IS user agreem't.

This User Agreement conforms to DoD Standard Notice and Consent Banner and User Agreement – JTF-GNO CTO 08-008A, May 9, 2008.

Fixes:

DB-DG0179-Generic (Manual)

Configure the warning banner to meet current DoD policy requirements.

Vulnerability Key: V0015122

STIG ID: DG0186

Release Number: 8

Status: Active

Short Name: DBMS network perimeter protection

Long Name: The database should not be directly accessible from public or unauthorized networks.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0186-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Databases often store critical and/or sensitive information used by the organization. For this reason, databases are targeted for attacks by malicious users. Additional protections provided by network defenses that limit accessibility help protect the database and its data from unnecessary exposure and risk.

Default

Finding Details: The database is directly accessible from public or unauthorized networks.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation EBBD-1, EBBD-2

Checks: DB-DG0186-Generic (Interview)

Review the System Security Plan to determine if the DBMS serves data to users or applications outside the local enclave.

If the DBMS is not accessed outside of the local enclave, this check is Not a Finding.

If the DBMS serves applications available from a public network (e.g. the Internet), then confirm that the application servers are located in a DMZ.

If the DBMS is located inside the local enclave and is directly accessible to public users, this is a Finding.

If the DBMS serves public-facing applications and is not protected from direct client connections and unauthorized networks, this is a Finding.

If the DBMS serves public-facing applications and contains sensitive or classified information, this is a Finding.

Fixes: DB-DG0186-Generic (Manual)

Do not allow direct connections from users originating from the Internet or other public network to the DBMS.

Include in the System Security Plan for the system whether the DBMS serves public-facing applications or applications serving users from other untrusted networks.

Do not store sensitive or classified data on a DBMS server that serves public-facing applications.

Vulnerability Key: V0015121

STIG ID: DG0187

Release Number: 7

Status: Active

Short Name: DBMS software file backups

Long Name: DBMS software libraries should be periodically backed up.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC /

--	--	--	--

Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0187-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The DBMS application depends upon the availability and integrity of its software libraries. Without backups, compromise or loss of the software libraries can prevent a successful recovery of DBMS operations.

Default Finding Details: DBMS software libraries are not periodically backed up.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation COSW-1

Checks: DB-DG0187-Generic (Interview)
Review the System Security Plan for a list of all DBMS application software libraries and third-party database applications to be included in software library backups with the DBA.

Review evidence of inclusion of the library in current backup records.

If any software library files are not included in regular backups, this is a Finding.

Fixes: DB-DG0187-Generic (Manual)
Configure backups to include all DBMS application and third-party database application software libraries.

Vulnerability Key: V0015154

STIG ID: DG0190

Release Number: 6

Status: Active

Short Name: DBMS remote system credential use and access

Long Name: Credentials stored and used by the DBMS to access remote databases or applications should be authorized and restricted to authorized users.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0190-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Credentials defined for access to remote databases or applications may provide unauthorized access to additional databases and applications to unauthorized or malicious users.

Default Finding Details: Credentials stored and used by the DBMS to access remote databases or applications are not authorized or restricted to authorized users.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0190-Generic (Interview)

Review the list of defined database links generated from the DBMS. Compare to the list in the System Security Plan with the DBA.

If no database links are listed in the database and in the System Security Plan, this check is Not a Finding.

If any database links are defined in the DBMS, verify the authorization for the definition in the System Security Plan.

If any database links exist that are not authorized or not listed in the System Security Plan, this is a Finding.

Fixes: DB-DG0190-Generic (Manual)

Grant access to database links to authorized users or applications only.

Document all database links access authorizations in the System Security Plan.

Vulnerability Key: V0015660

STIG ID: DG0192

Release Number: 4

Status: Active

Short Name: DBMS fully-qualified name for remote access

Long Name: Remote database or other external access should use fully-qualified names.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--------------------------------------------------------------------------------------------------------------------	------------------------------

☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0192-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Use of unqualified names may lead to connections to unintended targets. Fully-qualified names or names that specify the entire hierarchical classification to a unique global name can help to prevent unintentional connections to potentially malicious or dangerous systems.

Default Finding Details: Remote database or other external access do not use fully-qualified names.

Documentable: No

Documentable Explanation:

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation DCFA-1

Checks: DB-DG0192-Generic (Manual)
Review any certificates used by the DBMS to identify remote systems.

If the certificate name does not indicate the fully-qualified name of the server, that is, a hierarchically complete name that includes a minimum of domain and server name, this is a Finding.

Fixes: DB-DG0192-Generic (Manual)
Specify the fully-qualified name of the server in all connection definitions.

Vulnerability Key: V0015108

STIG ID: DG0194

Release Number: 8

Status: Active

Short Name: DBMS developer privilege monitoring on shared DBMS

Long Name: Privileges assigned to developers on shared production and development DBMS hosts and the DBMS should be monitored every three months or more frequently for unauthorized changes.

☐ Open
☐ Not a Finding
☐ Not Applicable

Comments:

☐ Not Reviewed

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0194-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: The developer role does not require Need-to-Know or administrative privileges to production databases. Assigning excess privileges can lead to unauthorized access to sensitive data or compromise of database operations.

Default Finding Details: Privileges assigned to developers on shared production and development DBMS hosts and the DBMS are not monitored every three months or more frequently for unauthorized changes.

Documentable: No

Documentable Explanation:

Responsibility: Information Assurance Officer

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECPC-1, ECPC-2

Checks: DB-DG0194-Generic (Interview)

If the DBMS or DBMS host is not shared by production and development activities, this check is Not a Finding.

Review policy, monitoring procedures and evidence of developer privileges on shared development and production DBMS and DBMS host systems with the IAO.

If developer privileges are not monitored every three months or more frequently, this is a Finding.

NOTE: Though shared production/non-production DBMS installations was allowed under previous database STIG guidance, doing so may place it in violation of OS, Application, Network or Enclave STIG guidance. Ensure that any shared production/non-production DBMS installations meets STIG guidance requirements at all levels or mitigate any conflicts in STIG guidance with your DAA.

Fixes: DB-DG0194-Generic (Manual)

Develop, document and implement policy and procedures to monitor DBMS and DBMS host privileges assigned to developers on shared production and development systems to detect unauthorized assignments every three months or more often.

Recommend establishing a dedicated DBMS host for production DBMS installations (See Checks DG0109 and DG0110). A dedicated host system in this case refers to an instance of the operating system at a minimum. The operating system may reside on a virtual host machine where supported by the DBMS vendor.

Vulnerability Key: V0015109

STIG ID: DG0195

Release Number: 8

Status: Active

Short Name: DBMS host file privileges assigned to developers

Long Name: DBMS production application and data directories should be protected from developers on shared production/development DBMS host systems.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

STIG ID: DG0195-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion: Developer roles should not be assigned DBMS administrative privileges to production DBMS application and data directories. The separation of production and development DBA and developer roles help protect the production system from unauthorized, malicious or unintentional interruption due to development activities.

Default Finding Details: DBMS production application and data directories are not protected from developers on shared production/development DBMS host systems.

Documentable: No

Documentable Explanation:

Responsibility: System Administrator
Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation ECPC-1, ECPC-2

Checks: DB-DG0195-Generic (Interview)

If the DBMS host does not support both production and development operations, this check is Not a Finding.

Review the list of OS DBA group membership with the SA and DBA. Compare to the list in the System Security Plan.

If any accounts not identified in the System Security Plan for the production DBMS have been assigned DBA privileges (to include developer accounts), this is a Finding.

If OS DBA group membership is not included in the System Security Plan, this is a Finding.

NOTE: Though shared production/non-production DBMS installations was allowed under previous database STIG guidance, doing so may place it in violation of OS, Application, Network or Enclave STIG guidance. Ensure that any shared production/non-production DBMS installations meets STIG guidance requirements at all levels or mitigate any conflicts in STIG guidance with your DAA.

Fixes:

DB-DG0195-Generic (Manual)

Create separate DBMS host OS groups for developer and production DBAs.

Do not assign production DBA accounts to development OS groups. Do not assign development DBA accounts to production OS groups.

Remove any unauthorized accounts from both production and development OS groups.

Document authorized assignments in the System Security Plan.

Recommend establishing a dedicated DBMS host for production DBMS installations (See Checks DG0109 and DG0110). A dedicated host system in this case refers to an instance of the operating system at a minimum. The operating system may reside on a virtual host machine where supported by the DBMS vendor.

Vulnerability Key: V0015662

STIG ID: DG0198

Release Number: 8

Status: Active

Short Name: DBMS remote administration encryption

Long Name: Remote administration of the DBMS should be restricted to known, dedicated and encrypted network addresses and ports.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

Condition: Generic Database Installation (Target: Generic Database Installation)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

STIG ID: DG0198-Generic

Severity: Category II

Severity Override Guidance:

Vulnerability Discussion:

Remote administration provides many conveniences that can assist in the maintenance of the designed security posture of the DBMS. On the other hand, remote administration of the database also provides malicious users the ability to access from the network a highly privileged function. Remote administration needs to be carefully considered and used only when sufficient protections against its abuse can be applied. Encryption and dedication of ports to access remote

administration functions can help prevent unauthorized access to it.

**Default
Finding
Details:**

Remote administration of the DBMS is not restricted to known, dedicated and encrypted network addresses and ports.

Documentable: No

**Documentable
Explanation:**

Responsibility: Database Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran App. A, Enclosure A, Para.5.b (8)
Department of Defense (DOD) Directive 8500.1, Information Assurance Para 4.18
Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation EBRP-1

Checks:

DB-DG0198-Generic (Interview)

If remote administration is disabled or not configured, this check is Not a Finding.

Review configured network access interfaces for remote DBMS administration with the SA and DBA.

These may be host-based encryptions such as IPSec or may be configured for the DBMS as part of the network communications and/or in the DBMS listening process.

For DBMS listeners, verify that encrypted ports exist and are restricted to specific network addresses to access the DBMS.

View the System Security Plan to review the authorized procedures and access for remote administration.

If the configuration does not match the documented plan, this is a Finding.

Fixes:

DB-DG0198-Generic (Manual)

Disable remote administration where it is not required or authorized.

Consider restricting administrative access to local connections only.

Where necessary, configure the DBMS network communications to provide an encrypted, dedicated port for remote administration access.

Develop and provide procedures for remote administrative access to DBAs that have been authorized for remote administration.

Verify during audit reviews that DBAs do not access the database remotely except through the dedicated and encrypted port.

Vulnerability Count - 103