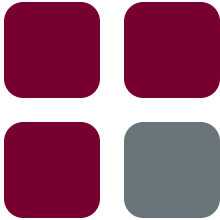


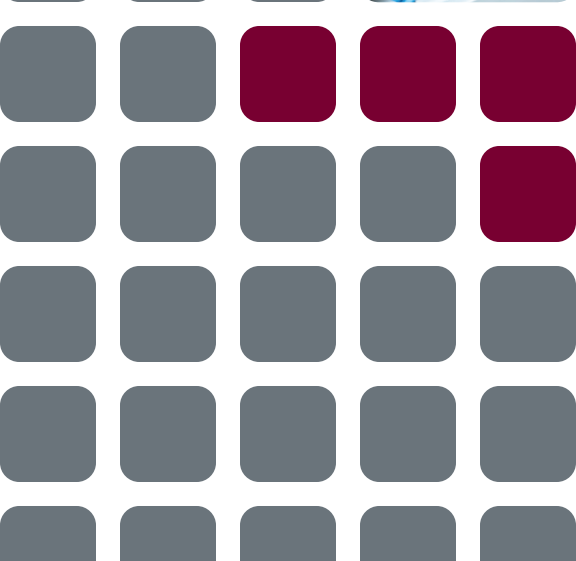
**APPLICATION  
SECURITY, INC.**  
Database Security, Risk and Compliance



# DbProtect™

Compliance Pack  
for the DISA STIG

Sample Guide



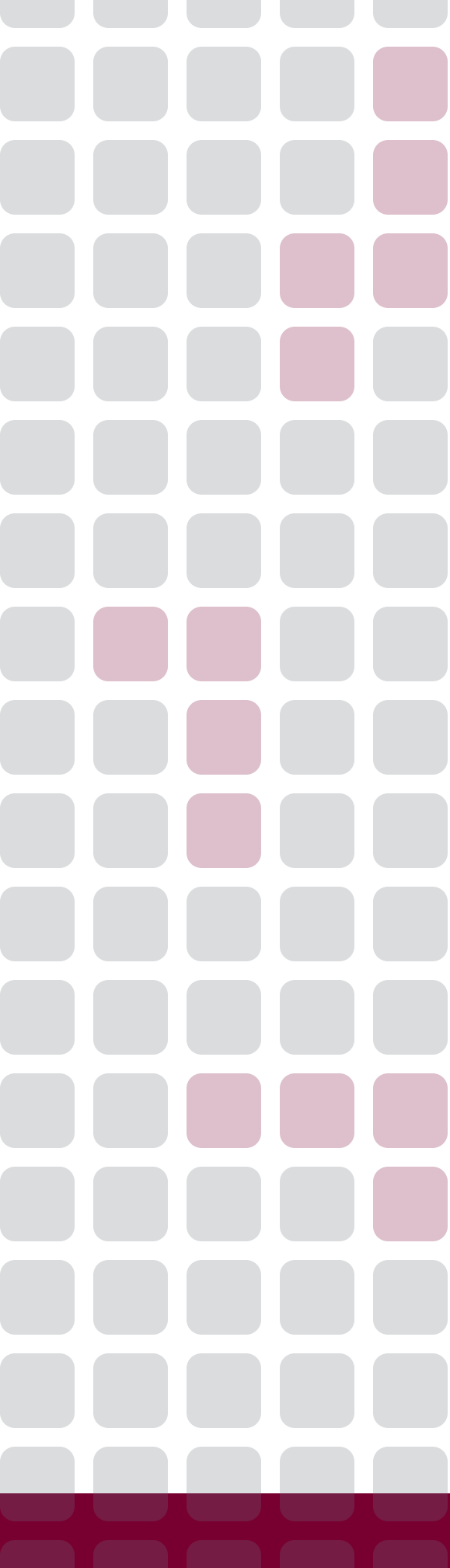


# DbProtect™

## Compliance Pack for the DISA STIG

### Contents

<b>Overview .....</b>	<b>4</b>
<b>General Capabilities .....</b>	<b>5</b>
Dashboard Drill-Through.....	5
Data Filtering .....	6
Multiple Report Formats .....	6
Report Distribution .....	6
<b>Dashboards .....</b>	<b>8</b>
Security Readiness Review .....	9
Security Readiness Review Trends.....	10
Compliance Heatmap .....	11
Top 10 STIG Findings .....	12
<b>Reports.....</b>	<b>13</b>
DISA STIG Findings - Summary .....	14
DISA STIG Findings - Detail.....	15
DISA STIG Findings - Affected Databases .....	16
DISA STIG Top Findings .....	17
DISA STIG Checklist Mapping .....	18
<b>About Application Security, Inc. ....</b>	<b>19</b>



## OVERVIEW

The Compliance Pack for the DISA STIG is an add-on analytics component to DbProtect. The Compliance Pack is a package of dashboards and reports that map Vulnerability Management findings to the language (the controls or checks) of the DISA STIG database checklists. This Compliance Pack makes it easy and clear to see how well your database environment measures up to the checklist.

The Security Technical Implementation Guides (STIG) is authored by the U.S. Department of Defense's Defense Information Systems Agency to provide strong specific guidance for the secure configuration of the systems retaining DoD information. Implementation of this technical guidance provides risk assurance to meet the standards prescribed under the National Institute of Standards and Technology's (NIST) authority and to meet the requirements of the Federal Information Security Management Act (FISMA). Besides being utilized in the U.S. Government, the DISA STIG has been adopted for use in the corporate business sector.

The Compliance Pack provides top-line indicators to quickly ascertain your environment's compliance to the DISA STIG. The Compliance Pack will remain up-to-date with changes to the DISA STIG so you do not have to.

## GENERAL CAPABILITIES

The Compliance Pack for the DISA STIG will stay current with STIG updates.

### Dashboard Drill-Through

- Dashboards provide top-line indicators of security risk posture.
- Dashboards are interactive and can be drilled-into to get more detailed information.

#### DISA STIG Premium Content Pack

Reporting on  
■ Microsoft SQL Server 217  
■ Oracle 27

#### Security Readiness Review

For all Assets As of May 24, 2011 10:59:16 PM

Provides the current snapshot of the database inventory evaluated against the DISA STIG checklists.

■ Open Finding  
 ■ Not a Finding  
 ■ Not Reviewed

#### Security Readiness Review Trends

For all Assets As of May 24, 2011 10:59:20 PM

Presents historical data points of successfully passed checks. Downward trends should be further investigated.

#### Compliance Heatmap

For all Assets As of May 24, 2011 10:59:10 PM

Databases are classified into compliance categories as:

- N/R - Database not reviewed
- 0% - All STIGs failed to run
- 25% - Includes at least a CAT-1 finding
- 50% - Includes at least a CAT-2 finding
- 75% - Includes at least a CAT-3 finding
- 100% - Reviewed and no findings

■ << Not Compliant  
 ■ 0 %  
 ■ 25 %  
 ■ 50 %  
 ■ 75 %  
 ■ 100 %  
 >> Compliant

#### Top 10 STIG Findings

For all Assets As of May 24, 2011 10:59:09 PM

Lists the most pervasive findings that are found on the most databases.

Rank	STIG ID	Severity	Short Name	Databases w/ Finding
1	DG0121	Category II	DBMS application user privilege assignment	9
2	DM1715	Category II	Unauthorized object permission grants	9
3	DG0003	Category II	DBMS security patch level	7
4	DG0014	Category II	DBMS demonstration and sample databases	7
5	DG0123	Category II	DBMS Administrative data access	7
6	DM1709	Category II	Guest user	7
7	DM2119	Category II	Registry extended stored procedures access	7
8	DM3566	Category II	Authentication mode	7
9	DG0029	Category II	Database auditing	6
10	DG0030	Category II	DBMS audit data maintenance	6

See: [full list](#)

#### Reports

- [DISA STIG Findings - Summary](#)
- [DISA STIG Findings - Detail](#)
- [DISA STIG Checklist Mapping \(Microsoft SQL Server\)](#)
- [DISA STIG Checklist Mapping \(Oracle\)](#)
- [DISA STIG Policy for Vulnerability Management](#)
- [DISA STIG Version Mapping](#)
- [DISA STIG Findings - Detail \(XML\)](#)

#### References

- [Database Security Checklists](#)

## GENERAL CAPABILITIES (Cont.)

### Data Filtering

Many reports can be filtered to narrow the results to the specific system or class of findings.

### Multiple Report Formats

Each report supports the export to various output formats. Supported formats include:

- **MS Word** – This report offers the results in an easy-to-edit document for further customization.
- **PDF** – This report is presentation-ready in the popular Adobe format.
- **HTML** – This report is optimized for online viewing.
- **MS Excel** - Use this report to conduct additional data analyses or to create custom graphs in Excel.
- **Raw Data** - The complete raw data set is always available in CSV format for deeper analysis.

### Report Distribution

The additional reports provided by the Compliance Pack are integrated into the job scheduling capabilities of DbProtect's Vulnerability Management system. It offers the ability to automatically schedule and distribute a subset of available reports, eliminating unnecessary manual effort. Reports can be distributed:

- Daily, Weekly, Monthly, Quarterly, etc.

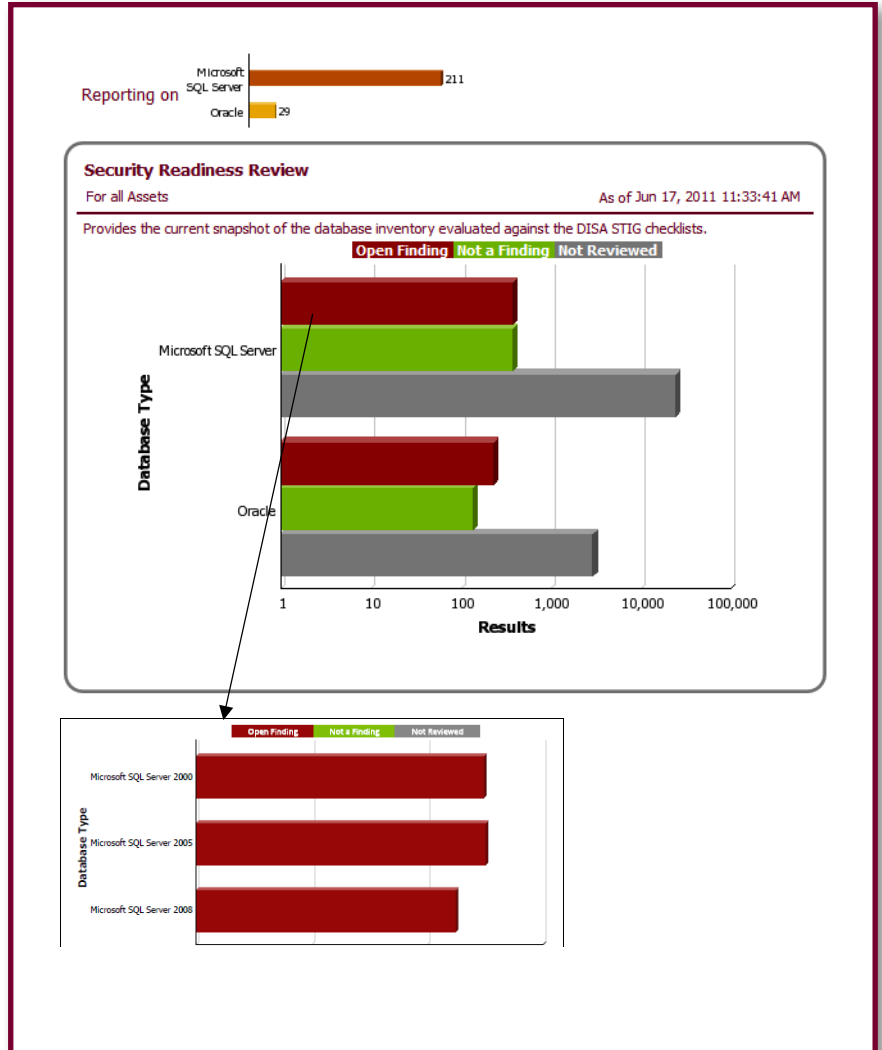


## DASHBOARD

The Compliance Pack includes a predefined security dashboard designed to provide your organization with a rapid and high-level view of database security measured by the DISA STIG.

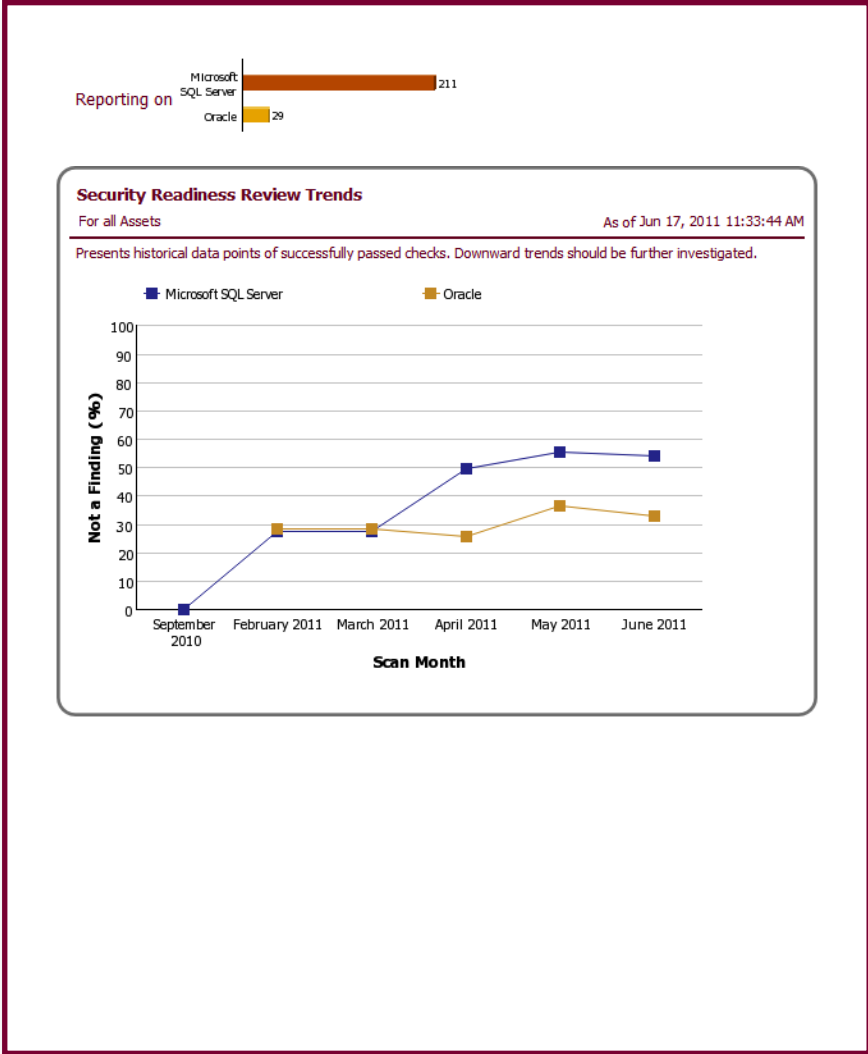
## SECURITY READINESS REVIEW

Provides a pass/fail snapshot of the overall database environment. Red results are negative results that indicate a finding has been uncovered. Green results are positive and indicate that a system passed a check. Grey results are indicators that a check evaluation has not yet occurred.



**SECURITY  
READINESS REVIEW  
TRENDS**

The trend lines help to evaluate how successful your organization has been in eliminating findings over time.



## COMPLIANCE HEATMAP

The Compliance Heatmap provides a snapshot of the compliance level of each database system. A system is rated with a percentage based on existing assessment results.

The scoring is categorized as:

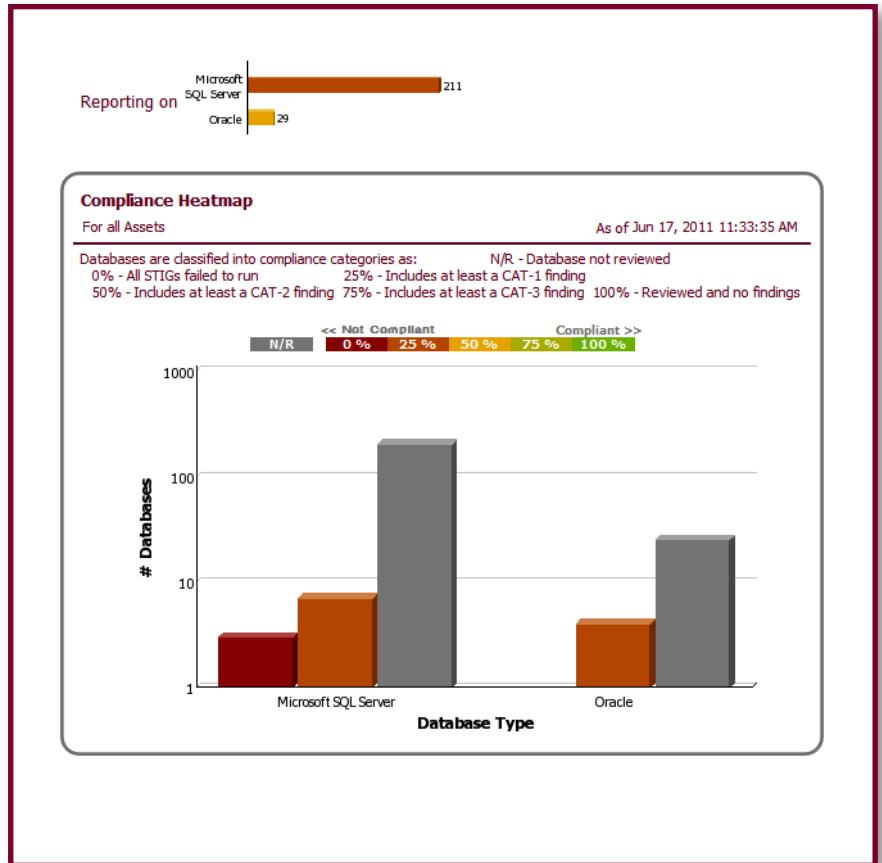
100% - Reviewed and no findings

75% - Reviewed and includes at worse a CAT-3 finding

50% - Reviewed and includes at worse a CAT-2 finding

25% - Reviewed and includes at least a CAT-1 finding

0% - A full review was not completed due to errors



## TOP 10 STIG FINDINGS

The issues that are most frequently affecting the database systems are highlighted by this list.

### Top 10 STIG Findings

For all Assets

As of Jun 17, 2011 11:33:32 AM

Lists the most pervasive findings that are found on the most databases.

Rank	STIG ID	Severity	Short Name	Databases w/ Finding
1	<a href="#">DG0121</a>	⚠️ Category II	<a href="#">DBMS application user privilege assignment</a>	15
2	<a href="#">DG0014</a>	⚠️ Category II	<a href="#">DBMS demonstration and sample databases</a>	13
3	<a href="#">DG0123</a>	⚠️ Category II	<a href="#">DBMS Administrative data access</a>	13
4	<a href="#">DM1715</a>	⚠️ Category II	<a href="#">Unauthorized object permission grants</a>	11
5	<a href="#">DG0102</a>	⚠️ Category II	<a href="#">DBMS services dedicated custom account</a>	10
6	<a href="#">DG0029</a>	⚠️ Category II	<a href="#">Database auditing</a>	9
7	<a href="#">DG0116</a>	⚠️ Category II	<a href="#">DBMS privileged role assignments</a>	9
8	<a href="#">DG0133</a>	⚠️ Category II	<a href="#">DBMS Account lock time</a>	9
9	<a href="#">DM1709</a>	⚠️ Category II	<a href="#">Guest user</a>	9
10	<a href="#">DM2119</a>	⚠️ Category II	<a href="#">Registry extended stored procedures access</a>	9

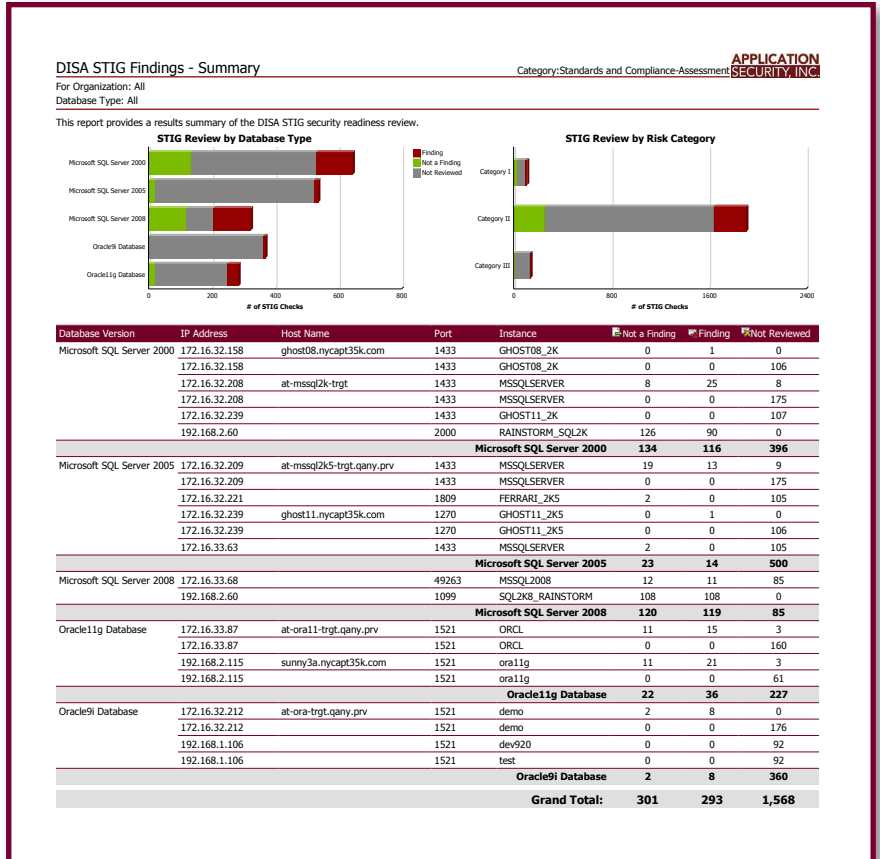
See: [full list](#)

## REPORTS

The Compliance Pack adds additional reports to DbProtect that can be generated as part of scheduled assessment jobs, through the manifest of reports in Analytics & Reporting, or interactively by drilling-through the charts in the dashboard.

## STIG FINDINGS - SUMMARY

The summary report provides a quick high level status of pass/fail for each database system.



**DISA STIG FINDINGS - DETAIL**

The detailed report provides the complete list of results per database system. The printed version of the report includes a table of contents for easy navigation. Charts are provided to provide high-level views of the results. The detailed results will include whether a check pass or failed, and include details on why a check was included as finding.

**APPLICATION SECURITY, INC.**

**DISA STIG Findings - Detail** Category: Standards and Compliance-Assessment

For Organization: All  
 Database Version: Microsoft SQL Server 2008  
 Compliance Level: 0%

---

This report shows the detailed results of a DISA STIG security readiness review. The checks that have been tested will be marked as either an "Open Finding" or "Not a Finding". Checks that require manual investigation or have not been tested are designated as "Not Reviewed".

**Table of Contents**

**Charts** ..... 2

    STIG Review By Database Type ..... 2

    STIG Review By Risk Category ..... 2

**Assets** ..... 2

    Microsoft SQL Server 2008 ..... 2

**STIG Review By Database Type**

**STIG Review By Risk Category**

**Microsoft SQL Server 2008**

Database: - 172.16.33.68 : 49263 - MSSQL2008

Not a Finding: 12

STIG ID	VKEY	Severity	STIG Description	Detail
DG0001	V0005658	Category I	The version of MS SQL Server must be listed by Microsoft as a supported version. Microsoft discontinues fixes for unsupported versions on reported dates. In order to maintain a secure environment, the installed version must continue to receive fixes for reported vulnerabilities.	
DG0002	V0004758	Category II	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.	
DG0128	V0015635	Category I	DBMS default passwords provide a commonly known and exploited means for unauthorized access to database installations.	

Use is indicated and authorized.

Open Finding: 11

STIG ID	VKEY	Severity	STIG Description	Detail
DG0003	V0005659	Category II	Maintaining the currency of the software version protects the database from known vulnerabilities.	[Latest Hotfix: 10.0.4000.0] [Database Version: 10.0.1600.22]
DG0014	V0015609	Category II	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.	[Database:AdventureWorks]
DG0121	V0015629	Category II	Privileges granted outside the role of the application user job function are more likely to go unmanaged or without oversight for authorization. Maintenance of privileges using roles defined for discrete job functions offers improved oversight of application user privilege assignments and helps to protect against unauthorized privilege assignment.	[Granted By:dbo] [Permission:EXECUTE] [Database:master] [Granted To: #MS_AgentSigningCertificate#] [Class:DATABASE] [Granted To:ur] [Permission:EXECUTE] [Class:OBJECT_OR_COLUMN] [Database:master] [State:GRANT] [Schema Name:sys] [Granted By:dbo] [Object Name:sp_srvrolepermission] [Granted To: #MS_PolicyEventProcessingLogin#] [Permission:EXECUTE] [Class:OBJECT_OR_COLUMN] [Database:master] [State:GRANT] [Schema Name:sys] [Granted By:dbo] [Object Name:sp_syspolicy_execute_policy] [Granted To:aduser] [Permission:EXECUTE] [Class:OBJECT_OR_COLUMN] [Database:master] [State:GRANT] [Schema Name:sys] [Granted By:dbo] [Object Name:sp_helpprotect] [Granted To:aduser] [Permission:EXECUTE] [Class:OBJECT_OR_COLUMN] [Database:master] [State:GRANT] [Schema Name:sys] [Granted By:dbo] [Object Name:sp_helpuser] [Granted To:ur] [Permission:EXECUTE] [Class:OBJECT_OR_COLUMN]

**DISA STIG FINDING  
– AFFECTED  
DATABASES**

The Affected Databases report lists each of the database systems that have failed a specific check.

APPLICATION SECURITY, INC.

**DISA STIG Finding – Affected Databases** Category: Standards and Compliance-Assessment

For Organization: All  
 STIG ID: DG0121  
 STIG Short Name: DBMS application user privilege assignment  
 STIG Description: Privileges granted outside the role of the application user job function are more likely to go unmanaged or without oversight for authorization. Maintenance of privileges using roles defined for discrete job functions offers improved oversight of application user privilege assignments and helps to protect against unauthorized privilege assignment.

---





















**Affected Databases**

Database Version	# of Assets
Microsoft SQL Server 2000	4
Microsoft SQL Server 2005	2
Microsoft SQL Server 2008	3

Database Type	Database Version	Organization	IP Address	Port	Instance	Host
Microsoft SQL Server	Microsoft SQL Server 2000	AppDetectivePro	192.168.2.60	2000	RAINSTORM_SQL2K	
			172.16.32.208	1433	MSSQLSERVER	at-mssql2k-trgt
		AppSecInc	192.168.2.60	2000	RAINSTORM_SQL2K	
			172.16.32.208	1433	MSSQLSERVER	at-mssql2k-trgt
Microsoft SQL Server 2005	AppSecInc	172.16.32.209	1433	MSSQLSERVER	at-mssql2k5-trgt.qany.prv	
		172.16.32.209	1433	MSSQLSERVER	at-mssql2k5-trgt.qany.prv	
Microsoft SQL Server 2008	Microsoft SQL Server 2008	AppDetectivePro	192.168.2.60	1099	SQL2K8_RAINSTORM	
			172.16.33.68	49263	MSSQL2008	
			192.168.2.60	1099	SQL2K8_RAINSTORM	

## DISA STIG TOP FINDINGS

The Top Findings report lists each check that returned a finding in the database environment ranked by the number of databases it affects.

DISA STIG Top Findings					<b>APPLICATION SECURITY, INC.</b>
For Organization: All					
This report lists all the findings that are found on the databases.					
Rank	STIG ID	Severity	Short Name	Databases w/ Finding	
1	DG0121	 Category II	DBMS application user privilege assignment	9	
2	DM1715	 Category II	Unauthorized object permission grants	9	
3	DG0003	 Category II	DBMS security patch level	7	
4	DG0014	 Category II	DBMS demonstration and sample databases	7	
5	DG0123	 Category II	DBMS Administrative data access	7	
6	DM1709	 Category II	Guest user	7	
7	DM2119	 Category II	Registry extended stored procedures access	7	
8	DM3566	 Category II	Authentication mode	7	
9	DG0029	 Category II	Database auditing	6	
10	DG0030	 Category II	DBMS audit data maintenance	6	
11	DG0133	 Category II	DBMS Account lock time	6	
12	DM0510	 Category II	C2 audit mode	6	
13	DM3930	 Category II	Error log retention	6	
14	DG0032	 Category II	DBMS audit record access	5	
15	DG0073	 Category II	DBMS failed login account lock	5	
16	DG0125	 Category II	DBMS account password expiration	5	
17	DM0924	 Category II	SQL Server service account	5	
18	DM2142	 Category II	Remote access option	5	
19	DG0128	 Category I	DBMS default passwords	4	
20	DM1758	 Category I	xp_cmdshell option	4	

**DISA STIG CHECKLIST MAPPING**

The checklist mapping reports showcases the detailed mappings of DbProtect’s SHATTER Knowledgebase to the DISA STIG check identifiers.

This report can be used to get a better understanding of how DbProtect performs its assessments or to why a check will return a finding or not.

Depending on your environment, you may optionally modify your policy to include or exclude more checks.

APPLICATION SECURITY, INC.

**DISA STIG Checklist Mapping (Oracle)** Category: Standards and Compliance-Assessment

For Organization: All  
Database Type: Oracle

This report provides the mapping of the DISA STIG checks to the SHATTER Knowledgebase checks. This information is useful in understanding how the product performs its automated assessments. In some cases, a single DISA STIG check may be comprised of multiple SHATTER Knowledgebase checks. A DISA STIG check returns a finding if any of the mapped SHATTER Knowledgebase checks returns a finding or violation.

Database Type	STIG ID	Short Name	VULKEY	Severity	Description	SHATTER Check ID	SHATTER Check Name	SHATTER Check Type(Pen Test or Audit)	Checklist	References
Oracle	D03 847	Oracle spoolmain.log file	V00026 07	Category II	The spoolmain.log file is generated by the Database Configuration Assistant (DBCA) database management tool. This file may contain login passwords in clear text. Disclosure of this file to unauthorized persons provides login credentials to the privileged DBA account.	733	Database Creation SPOOLMAIN.LOG File	Audit	V8R1-7	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 Database Security Technical Implementation Guide 3.1.4.1
	DG0 001	DBMS version support	V00056 58	Category I	Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack.	628	No patches available for version	Audit	V8R1-8	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 VIM-1
	DG0 002	DBMS version upgrade plan	V00047 58	Category II	Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack. Developing and implementing	758	DBMS version upgrade plan	Audit		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

Generated using DISA-STIG Content Pack 1.0.27 with SHATTER KB 4.2.14719 on Jun 6, 2011 10:49:35 PM EDT  
 Powered by Application Security, Inc. Page 1 of 42 DbProtect - Complete Database Security

## ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: [www.appsecinc.com](http://www.appsecinc.com) | [www.teamshatter.com](http://www.teamshatter.com)

For a free database vulnerability assessment visit:  
[www.appsecinc.com/downloads/appdetectivepro](http://www.appsecinc.com/downloads/appdetectivepro)

Follow us on Twitter: [www.twitter.com/appsecinc](https://twitter.com/appsecinc) | [www.twitter.com/teamshatter](https://twitter.com/teamshatter)

**APPLICATION  
SECURITY, INC.**<sup>®</sup>  
[www.appsecinc.com](http://www.appsecinc.com)

350 Madison Avenue, 6th Floor, New York, NY 10017

TOLL FREE 866 9APPSEC MAIN +1 212 912 4100 FAX +1 212 947 8788