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

DATA SHEET

AppDetectivePro™ 7.0

The De-Facto Standard for Corporate Auditors and IT Advisors

By an overwhelming margin, corporate auditors, IT advisors, and Federal Government OIGs have made AppDetectivePro their database scanning and vulnerability assessment solution of choice. Deployed in over 130 countries, AppDetectivePro has been used to assess hundreds of thousands of databases in every vertical market. A thorough examination of the databases that store and process critical business information is a critical component of any IT audit; AppDetectivePro enables auditors and advisors to complete the task quickly, reliably, and cost effectively.

DATABASE SECURITY AND COMPLIANCE EFFORTS START WITH A SCAN

Manually assessing the security posture of a database is a complex task that requires expertise and significant resources. Manually measuring and demonstrating compliance with industry and government regulations is even more difficult. By equipping your staff with AppDetectivePro™, you will immediately and significantly reduce the complexity of these tasks. IT auditors and advisors, regardless of skill level, will be enabled to perform easy and repeatable database security assessments, capture all results for manual control checks, and generate compliance reports. AppDetectivePro leverages Application Security, Inc.'s SHATTER knowledgebase, the industry's most complete collection of database vulnerability and misconfiguration checks to ensure the most comprehensive database assessment possible. The solution consists of three distinct functional modules:

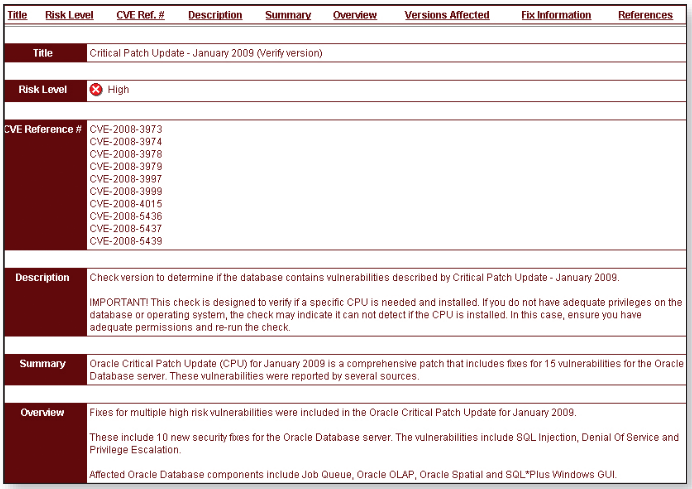
- Database Discovery
- Database Vulnerability Assessment
- User Rights Review

DATABASE DISCOVERY

The critical first step in any IT audit is to identify all assets and applications residing on the network. AppDetectivePro's Database Discovery module provides complete visibility into the inventory of databases on any network. Simply connect a laptop running AppDetectivePro to the network, and without agents, database logins, or other knowledge, the solution will scan and identify every database by vendor and release level.

DATABASE VULNERABILITY ASSESSMENT

AppDetectivePro has been the vulnerability assessment standard since the product was launched in 2002. With a policy-driven scanning engine, AppDetectivePro identifies vulnerabilities and misconfigurations. Issues identified include default or weak passwords, missing patches, poor access controls, and a host of other conditions. A flexible assessment framework allows auditors to choose between an outside-in, "hackers eye view" of the database which requires no credentials, or a more thorough inside-out scan which is facilitated through a read-only database account. AppDetectivePro includes built-in templates to satisfy the requirements of security best practices and various regulatory compliance initiatives. Compliance standards covered include: DISA STIG, NIST 800-53 (FISMA), PCI DSS, HIPAA, GLBA, Sarbanes-Oxley, ISO 27001, CoBIT, and Canada's MITS.



Title Risk Level CVE Ref. # Description Summary Overview Versions Affected Fix Information References

Title	Critical Patch Update - January 2009 (Verify version)
Risk Level	✗ High
CVE Reference #	CVE-2008-3973 CVE-2008-3974 CVE-2008-3978 CVE-2008-3979 CVE-2008-3997 CVE-2008-3999 CVE-2008-4015 CVE-2008-5436 CVE-2008-5437 CVE-2008-5439
Description	Check version to determine if the database contains vulnerabilities described by Critical Patch Update - January 2009. IMPORTANT! This check is designed to verify if a specific CPU is needed and installed. If you do not have adequate privileges on the database or operating system, the check may indicate it can not detect if the CPU is installed. In this case, ensure you have adequate permissions and re-run the check.
Summary	Oracle Critical Patch Update (CPU) for January 2009 is a comprehensive patch that includes fixes for 15 vulnerabilities for the Oracle Database server. These vulnerabilities were reported by several sources.
Overview	Fixes for multiple high risk vulnerabilities were included in the Oracle Critical Patch Update for January 2009. These include 10 new security fixes for the Oracle Database server. The vulnerabilities include SQL Injection, Denial Of Service and Privilege Escalation. Affected Oracle Database components include Job Queue, Oracle OLAP, Oracle Spatial and SQL*Plus Windows GUI.

Pen Test

AppDetectivePro's unique Pen Test scan provides the outside-in view of a database's security posture that is safe for use on production systems. The functionality does not perform intrusive tests or risky attack simulations. AppDetectivePro's Pen Test gathers a detailed view of vulnerabilities that could allow an outsider access into a database system and provides awareness to the organization before the vulnerabilities are exploited. The

Pen Tests are executed without the need to schedule downtime and can operate in a tight maintenance window. Pen Tests require no database login information or passwords. Point the application at any database, and within seconds, results will be delivered.

Security Audit

For a more detailed, "inside-out" perspective of vulnerabilities and a complete assessment of database configuration settings, AppDetectivePro offers its Audit scan. Audits require minimal access to the databases being scanned; a read-only account with no access to sensitive user data is all that is required to perform a complete analysis. Audits extend beyond the capabilities of a Pen Test, identifying all the security holes that could allow an outsider access to a database. In addition, audits provide a detailed view of potential avenues of insider privilege abuse. Insiders can abuse their privileges to gain inappropriate access to data or functionality. AppDetectivePro Audit scans allow, organizations to protect sensitive information residing in database applications, guard against unauthorized outsider and insider access, and seamlessly demonstrate compliance to relevant requirements.

KEY FEATURES:

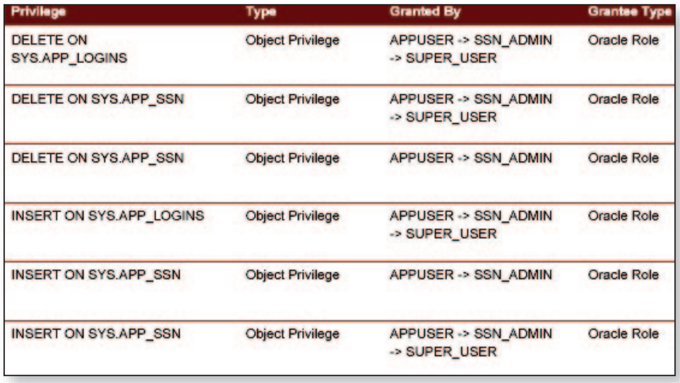
- **Automated database discovery and inventory**
- **Database-specific vulnerability assessment**
- **Compliance work plans and policies**
- **Industry leading database vulnerability knowledgebase**
- **Automated information gathering and analysis**
- **Concurrent database scanning**
- **Deep analysis of user and role permissions**
- **Advanced, customizable reporting**
- **Easy to deploy, configure and use**

Vulnerability Knowledgebase, Up-to-Date Support

AppDetectivePro is based on the industry's largest known collection of database-specific vulnerabilities. Compiled by Team SHATTER, Application Security, Inc.'s world-class threat research organization, the SHATTER knowledgebase is the most extensive set of database vulnerability and misconfiguration checks and rules on the market today. The knowledgebase is updated on a regular basis through Application Security, Inc.'s ASAP Updates, ensuring that the most recent vulnerabilities can be identified and remediated.

USER RIGHTS REVIEW

A key component of nearly every regulatory initiative that addresses protection of data is a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user's business function or need to know. Traditionally, auditors have been forced to perform this analysis for database systems manually, consuming up to two weeks per database and often resulting in incorrect or incomplete information. AppDetectivePro User Rights addresses this problem by providing a scan-based review of user entitlements that automatically determines each user's effective privileges. The automated User Rights Review signifcantly reduces the time and resources required to determine who has access to which data, what type of access rights they have (read, write, delete) and how they were granted that access.



Privilege	Type	Granted By	Grantee Type
DELETE ON SYS.APP_LOGINS	Object Privilege	APPUSER -> SSN_ADMIN -> SUPER_USER	Oracle Role
DELETE ON SYS.APP_SSN	Object Privilege	APPUSER -> SSN_ADMIN -> SUPER_USER	Oracle Role
DELETE ON SYS.APP_SSN	Object Privilege	APPUSER -> SSN_ADMIN	Oracle Role
INSERT ON SYS.APP_LOGINS	Object Privilege	APPUSER -> SSN_ADMIN -> SUPER_USER	Oracle Role
INSERT ON SYS.APP_SSN	Object Privilege	APPUSER -> SSN_ADMIN	Oracle Role
INSERT ON SYS.APP_SSN	Object Privilege	APPUSER -> SSN_ADMIN -> SUPER_USER	Oracle Role

WORK PLAN AND POLICY QUESTIONNAIRE

A thorough database assessment is more than just the scan. It consists of checking controls beyond database configurations and parameter settings. Understanding the business process, how the application interacts with the database, and procedural operations (like backup and audit log review policies) round out a complete database assessment. AppDetectivePro work plan management capabilities extends the auditor's ability to capture all control information formulated in a questionnaire. It allows auditors to input password policy controls, run scans against password parameters, and independently conclude if a control is within compliance or not.

APPDETECTIVEPRO REPORTING

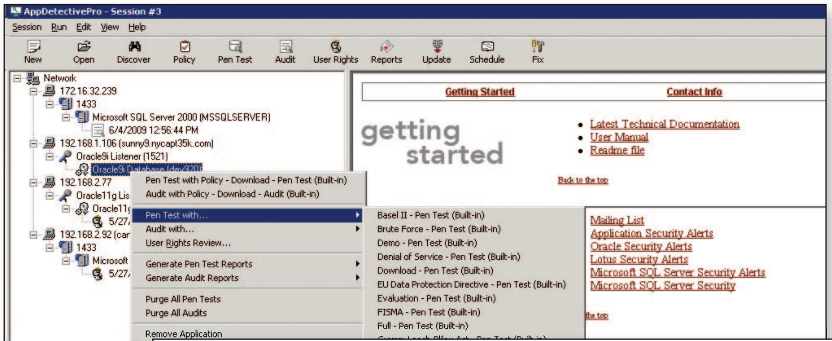
AppDetectivePro's reporting system allows organizations to easily report all database and application intelligence to appropriate stakeholders. Reporting options include: Inventory reports, Vulnerability Details and Summary reports, User Rights reports, Policy reports, and various others. Reports can be output in multiple formats including: PDF, Excel, Word, Crystal, HTML, XML and Text.

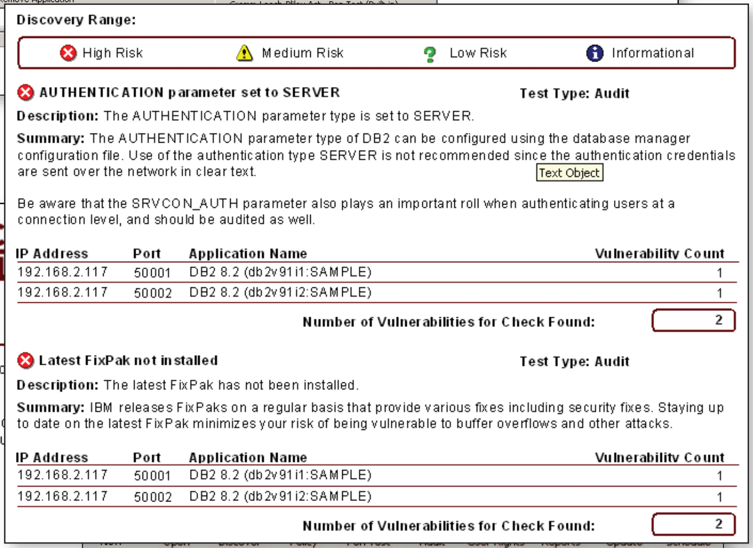
AppDetectivePro™

A 30-day evaluation copy of AppDetectivePro is available for download at: www.appsecinc.com/products/appdetective/

SYSTEM REQUIREMENTS

- **Operating System:** Microsoft Windows XP Professional SP2 or greater, Microsoft Windows Vista
- **Browser:** Internet Explorer version 7 or later
- **Processor:** 750 MHZ or 1 GHZ
- **RAM:** 1 GB or more
- **Hard Drive:** 300 MB of free disk space with additional space required to store vulnerability information
- **Database:** (Optional for storing AppDetectivePro results) Microsoft SQL Server 2008, 2005, 2000 or MSDE 2000 SP4


AppDetectivePro - Session #3
Session Run Edit View Help
New
Open
Discover
Policy
Pen Test
Audit
User Rights
Reports
Update
Schedule
Fix
Network
172.16.32.239
1433
Microsoft SQL Server 2000 (MSSQLSERVER)
6/4/2009 12:56:44 PM
192.168.1.106 (sunny9.nycapt35k.com)
Oracle9i Listener (1521)
Oracle9i Database (dev920)
192.168.2.77
Oracle11g Lis
Oracle11g
5/27/
192.168.2.92 (car
1433
Microsoft
5/27/
Pen Test with Policy - Download - Pen Test (Built-in)
Audit with Policy - Download - Audit (Built-in)
Pen Test with...
Audit with...
User Rights Review...
Generate Pen Test Reports
Generate Audit Reports
Purge All Pen Tests
Purge All Audits
Remove Application
Basel II - Pen Test (Built-in)
Brute Force - Pen Test (Built-in)
Demo - Pen Test (Built-in)
Denial of Service - Pen Test (Built-in)
Download - Pen Test (Built-in)
EU Data Protection Directive - Pen Test (Built-in)
Evaluation - Pen Test (Built-in)
FISMA - Pen Test (Built-in)
Full - Pen Test (Built-in)
Getting Started
Contact Info
getting started
Latest Technical Documentation
User Manual
Readme file
Back to the top
Mailing List
Application Security Alerts
Oracle Security Alerts
Lotus Security Alerts
Microsoft SQL Server Security Alerts
Microsoft SQL Server Security
the top
Risk Level



Discovery Range:

High Risk | Medium Risk | Low Risk | Informational

AUTHENTICATION parameter set to SERVER **Test Type: Audit**

Description: The AUTHENTICATION parameter type is set to SERVER.

Summary: The AUTHENTICATION parameter type of DB2 can be configured using the database manager configuration file. Use of the authentication type SERVER is not recommended since the authentication credentials are sent over the network in clear text. Text Object

Be aware that the SRVCON_AUTH parameter also plays an important roll when authenticating users at a connection level, and should be audited as well.

IP Address	Port	Application Name	Vulnerability Count
192.168.2.117	50001	DB2 8.2 (db2v91i1:SAMPLE)	1
192.168.2.117	50002	DB2 8.2 (db2v91i2:SAMPLE)	1

Number of Vulnerabilities for Check Found: 2

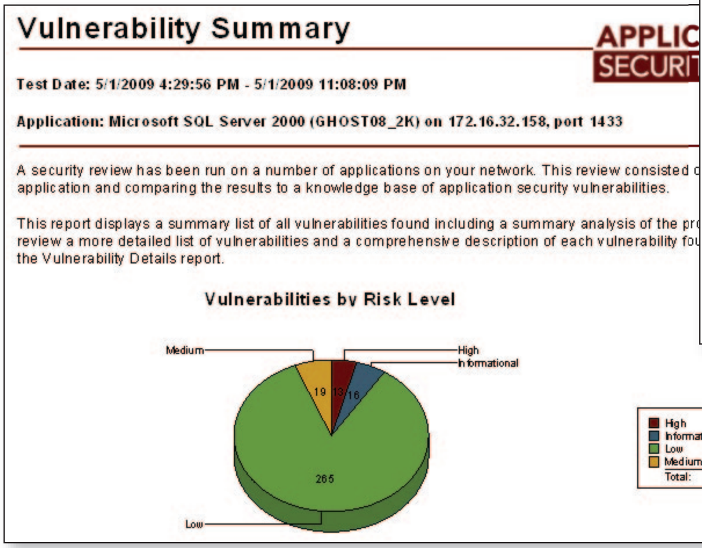
Latest FixPak not installed **Test Type: Audit**

Description: The latest FixPak has not been installed.

Summary: IBM releases FixPaks on a regular basis that provide various fixes including security fixes. Staying up to date on the latest FixPak minimizes your risk of being vulnerable to buffer overflows and other attacks.

IP Address	Port	Application Name	Vulnerability Count
192.168.2.117	50001	DB2 8.2 (db2v91i1:SAMPLE)	1
192.168.2.117	50002	DB2 8.2 (db2v91i2:SAMPLE)	1

Number of Vulnerabilities for Check Found: 2



Vulnerability Summary

APPLIC SECURI

Test Date: 5/1/2009 4:29:56 PM - 5/1/2009 11:08:09 PM

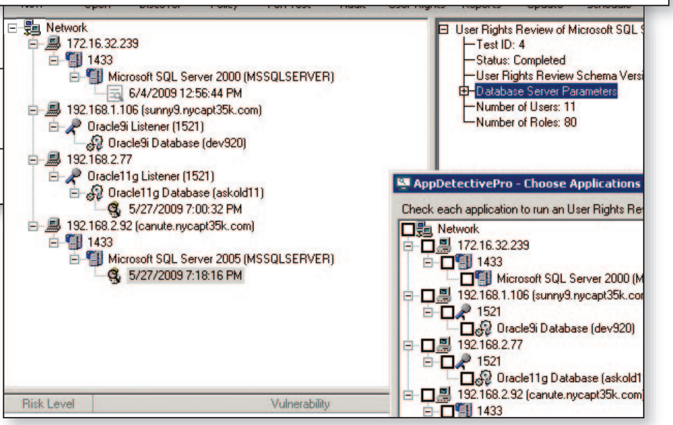
Application: Microsoft SQL Server 2000 (GHOST08_2K) on 172.16.32.158, port 1433

A security review has been run on a number of applications on your network. This review consisted o application and comparing the results to a knowledge base of application security vulnerabilities.

This report displays a summary list of all vulnerabilities found including a summary analysis of the pr review a more detailed list of vulnerabilities and a comprehensive description of each vulnerability fou the Vulnerability Details report.

Vulnerabilities by Risk Level

High	4.2%
Informational	5.1%
Low	84.7%
Medium	6.1%
Total:	100.0%


Network
172.16.32.239
1433
Microsoft SQL Server 2000 (MSSQLSERVER)
6/4/2009 12:56:44 PM
192.168.1.106 (sunny9.nycapt35k.com)
Oracle9i Listener (1521)
Oracle9i Database (dev920)
192.168.2.77
Oracle11g Listener (1521)
Oracle11g Database (askold11)
5/27/2009 7:00:32 PM
192.168.2.92 (canute.nycapt35k.com)
1433
Microsoft SQL Server 2005 (MSSQLSERVER)
5/27/2009 7:18:16 PM
Risk Level
Vulnerability
User Rights Review of Microsoft SQL S
Test ID: 4
Status: Completed
User Rights Review Schema Versi
Database Server Parameters
Number of Users: 11
Number of Roles: 80
AppDetectivePro - Choose Applications
Check each application to run an User Rights Re
Network
172.16.32.239
1433
Microsoft SQL Server 2000 (M
192.168.1.106 (sunny9.nycapt35k.co
1521
Oracle9i Database (dev920)
192.168.2.77
1521
Oracle11g Database (askold1
192.168.2.92 (canute.nycapt35k.com)
1433

AppDetectivePro enables auditors, IT advisors, security personnel and database administrators to implement database security, risk, and compliance best practices by continuously tracking and managing database vulnerabilities. With robust reporting capabilities and a customizable work plan manager and policy editor, AppDetectivePro arms enterprises with ready to deploy technology to manage security risk and extend compliance policies to the database.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

Application Security, Inc. is the leading provider of cross platform database security, risk and compliance solutions for the enterprise. Application Security, Inc.'s products – AppDetetectivePro and DbProtect – deliver the industry's most comprehensive database security solution and are used around the world in the most demanding environments by over 2,000 customers. The company was named to Inc. Magazine's 2007 (Inc. 500) and 2008 list of America's Fastest Growing Private Companies, and was also named to the 2008 Deloitte Technology Fast 50 by Deloitte & Touche. For more information, please visit www.appsecinc.com.

APPLICATION SECURITY, INC.®
www.appsecinc.com