

# Oracle Critical Patch Updates Unwrapped

Stephen Kost  
Chief Technology Officer  
Integrigy Corporation

Session #330

# Agenda

- Background of Critical Patch Updates
- Vulnerabilities
- Patches
- Patching Strategy
- Questions

# Integrigy Overview

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

## Corporate Details

- Founded December 2001
- Privately Held
- Based in Chicago, Illinois

# Integrigy Background

- A database/ERP company and a security company
- **Integrigy bridges the gap between applications, databases, and security**
- **Extensive experience with Oracle**
- Integrigy has found more security bugs in Oracle ERP than anyone else inside or outside of Oracle
- **AppSentry** – Oracle E-Business Security Assessment Tool
- **Integrigy Consulting** – Security Assessment Services

# Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
<b>Critical Patch Update July 2008</b>	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> <li>▪ 2 Issues in Oracle RDBMS Authentication</li> <li>▪ 2 Oracle E-Business Suite vulnerabilities</li> </ul>
<b>Critical Patch Update April 2008</b>	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update July 2007</b>	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update October 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ Default configuration issues</li> </ul>
<b>Critical Patch Update July 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update April 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update Jan 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #68</b>	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> <li>▪ Buffer overflows</li> <li>▪ Listener information leakage</li> </ul>
<b>Oracle Security Alert #67</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>▪ 10 SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #56</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>▪ Buffer overflow in FNDWRR.exe</li> </ul>
<b>Oracle Security Alert #55</b>	11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ Multiple vulnerabilities in AOL/J Setup Test</li> <li>▪ Obtain sensitive information (valid session)</li> </ul>
<b>Oracle Security Alert #53</b>	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ No authentication in FNDIFS program</li> <li>▪ Retrieve any file from O/S</li> </ul>

# Oracle Critical Patch Updates

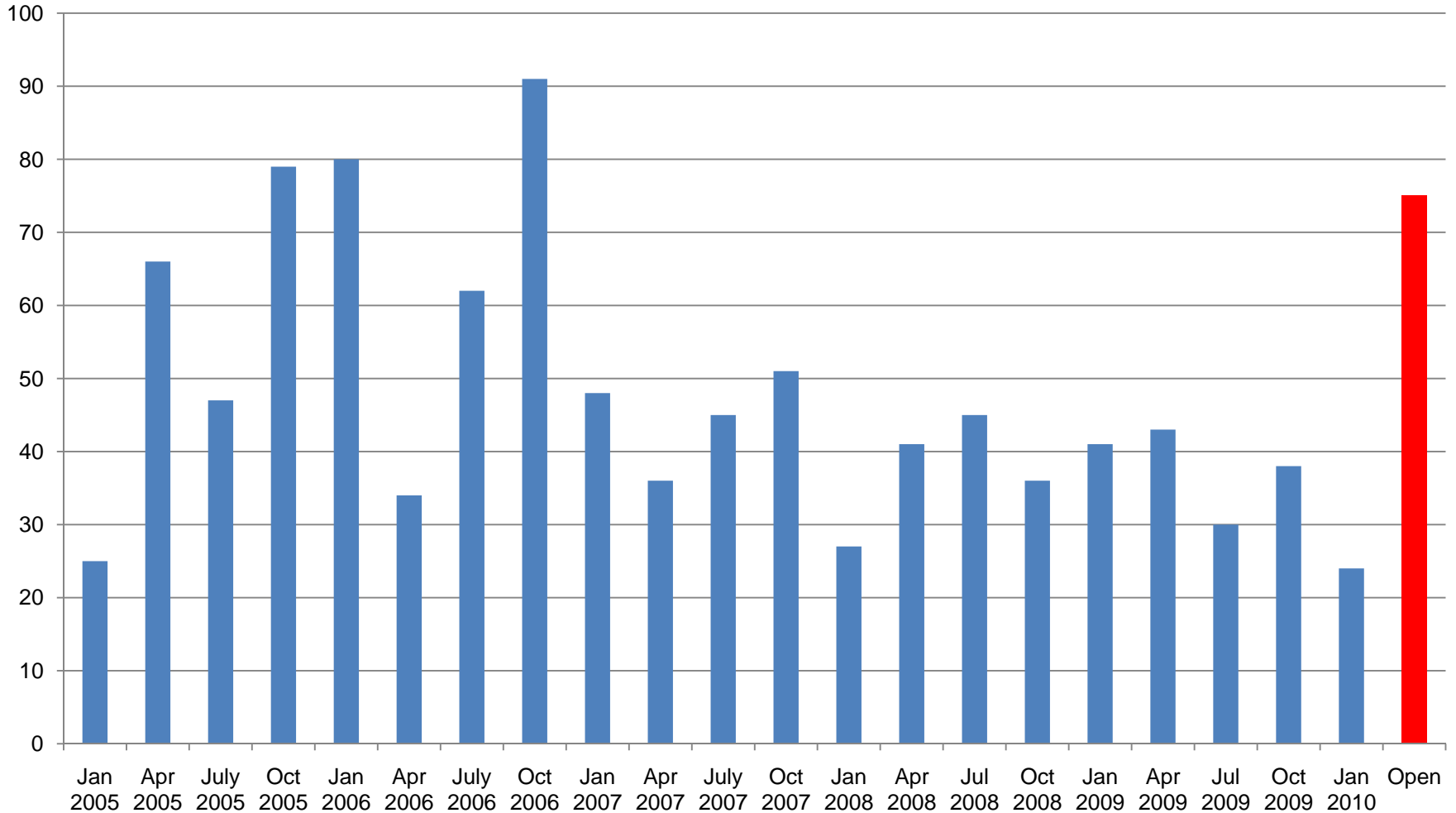
Fixes for security bugs in all Oracle products

- Released quarterly on a fixed schedule
- Tuesday closest to the 15th day of January, April, July and October
- Last CPU = **April 13, 2010**
- Next CPUs = **July 13, 2010** and **October 12, 2010**

**Twenty-one** CPUs released to date starting with Jan 2005

- 989 security bugs fixed (average is 47 bugs per CPU)
- 412 bugs in the Oracle Database
- 198 bugs in the Oracle E-Business Suite

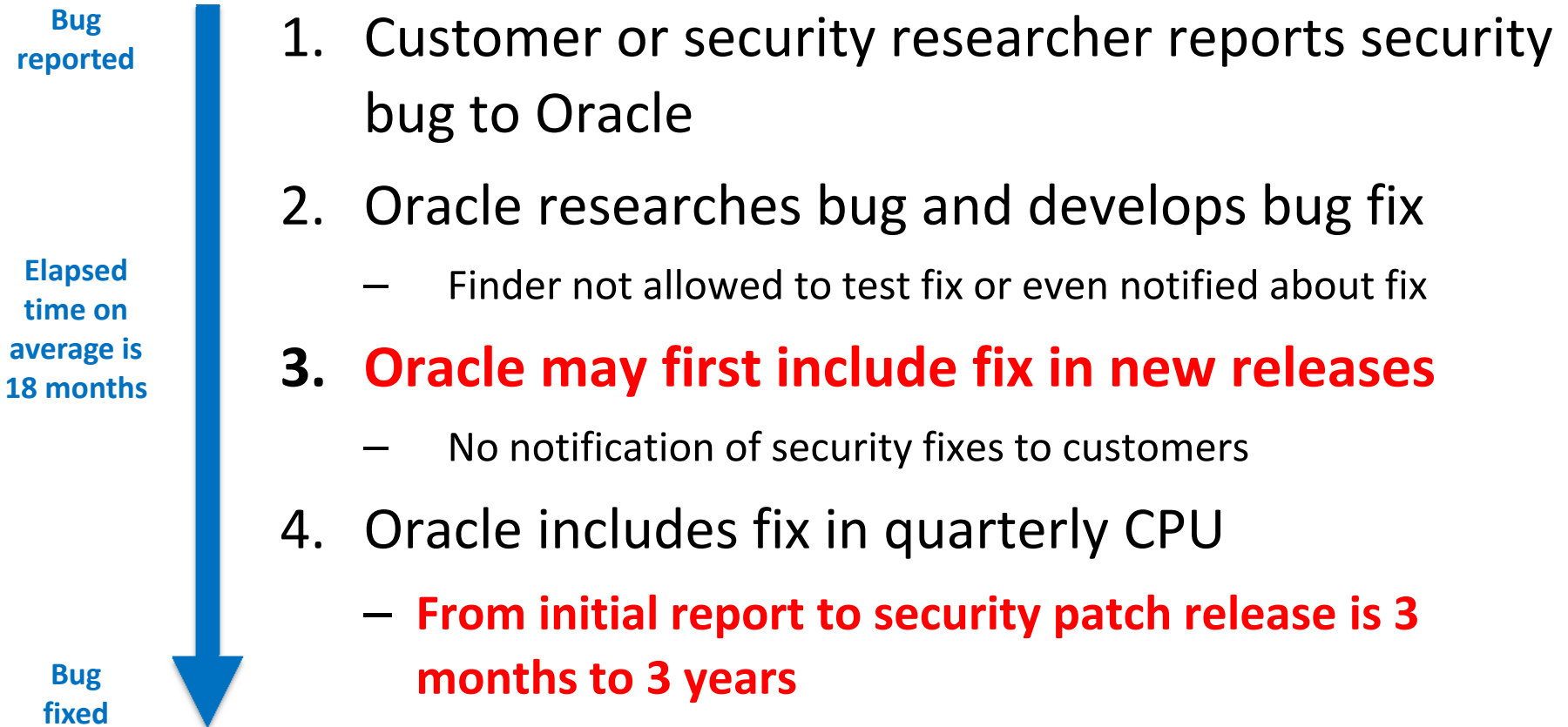
# Oracle Security Bugs per Quarter



# CPU Recent Changes

- Oracle Database Patch Setup Updates (PSU)
  - Introduced with July 2009 CPU
  - Critical Patch Update fixes + critical fixes
  - “Low Risk, High Content Value”
- Oracle E-Business Suite 11i Cumulative Patches
  - Introduced with January 2010 CPU
  - Supports 11.5.10 CU2 only

# Oracle Security Bug Process



# Oracle and CVSS

## CVSS = Common vulnerability Scoring System

- A common scoring for the risk and severity of vulnerabilities - base metric score is 1 to 10 (10=worst)
- Designed for network devices and servers, not databases and applications – biased toward root access

## ***Oracle CVSS base metric scores will always be low***

- A problem with the CVSS metric, not Oracle

Oracle Database realistic maximum is **5.5 to 6.5**

**Oracle includes “Partial+” in the advisory**

# % of Bugs Exploitable with No Auth

**10%**

# % of Bugs PUBLIC Exploitable

**48%**

For the CPUs January 2007 through January 2010 (95 of 197 database bugs)

## % of Published Exploits PUBLIC Exploitable

**78%**

For the CPUs January 2007 through January 2010 (29 of 37 database bugs)

***Who can exploit a PUBLIC bug?***

**Anyone with a  
database account**

*Remember those application accounts with generic passwords  
such as APPLSYSPUB/PUB in Oracle E-Business Suite*

# Database Vulnerabilities (Jan09)

Supported Database Version	<b>PUBLIC</b>	Other Advanced Privileges (i.e., EXECUTE_CATALOG_ROLE)
<b>9.2.0.8</b>	CVE-2008-5436 – OLAP CVE-2008-3974 – OLAPIMPL_T CVE-2008-3999 – OLAPIMPL_T	CVE-2008-5437 – DBMS_IJOB
<b>10.1.0.5</b>	CVE-2008-5436 – OLAP CVE-2008-3978 – Spatial CVE-2008-3979 – Spatial CVE-2008-3997 – DBMS_XSOQ_ODBO CVE-2008-3999 – OLAPIMPL_T	CVE-2008-5437 – DBMS_IJOB CVE-2008-4015 – DBMS_STREAMS_AUTH
<b>10.2.0.3</b> <b>10.2.0.4</b>	CVE-2008-5436 – OLAP CVE-2008-3979 – Spatial CVE-2008-3997 – DBMS_XSOQ_ODBO	CVE-2008-5437 – DBMS_IJOB
<b>11.1.0.6</b>		CVE-2008-5437 – DBMS_IJOB

# Vulnerability Demonstrations

1. Standard Oracle Database Package SQL Injection
2. Oracle Database Java 0-day Release at Black Hat DC 2010 – February 2, 2010

# Database Patches

- Database patches are cumulative for all previous Critical Patch Updates
  - Database patches include non-security fixes
  - Windows patches are really version upgrades
  - Testing should be similar to a version upgrade (i.e., 9.2.0.7 to 9.2.0.8)
  - Some Integrity clients now only do minimal testing
- Database patches provide the greatest security benefit – Apply them ASAP
  - Apply database patches now, other patches later
  - Otherwise, enable “Managed SQL\*Net Access” feature

# Oracle Database Patch Set Update

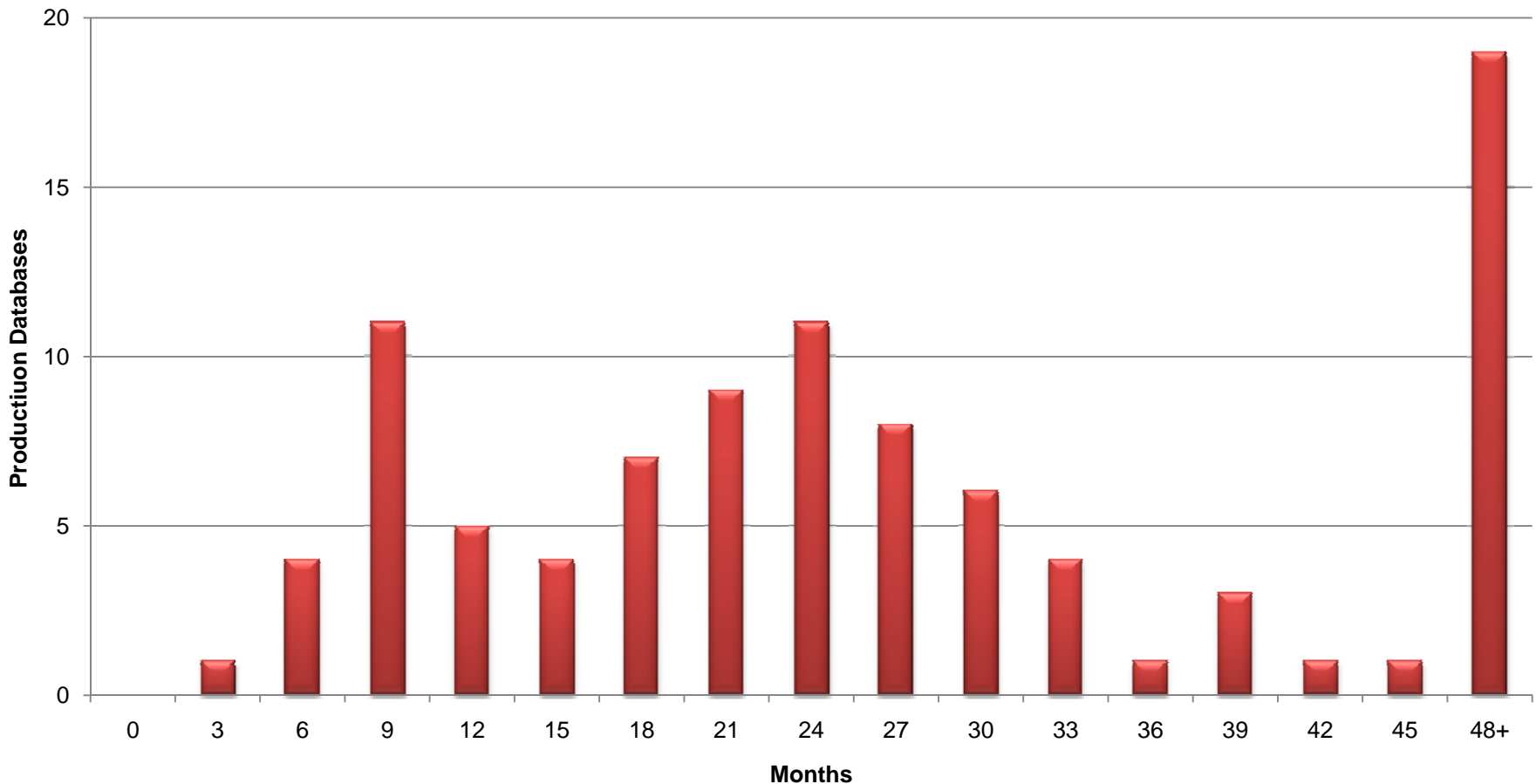
- Introduced with July 2009 CPU
- Critical Patch Update fixes + critical fixes
  - No configuration changes required
  - No execution changes (i.e., optimizer plans)
- Low-Risk, High-Value Content
- One Integrated, Well Tested Patch
- **Baseline Version for Easier Tracking**

# Oracle Database Patch Set Update

- January 2010 for 10.2.0.4 – Bug Fixes
  - CPU = 39
  - PSU = 149+
- Fully supported by Oracle E-Business
  - Not explicitly tested by EBS Development
- PSU is a patching path
  - **Once applied, must always apply PSUs rather than CPUs**
  - CPUs apply to base version only – no PSU

# Oracle CPU Patching Metric

## Security Patches - Months Behind



# SYS.REGISTRY\$HISTORY

- Since January 2006, contains 1 row for most recent CPU patch applied
  - Previous rows removed
- Semi-reliable method for determining if CPU patch is applied
  - Inconsistent across versions
  - Maybe removed if CPU is rolled back

```
SQL> SELECT comments, action_time,  
       id "PATCH_NUMBER", version  
FROM sys.registry$history  
WHERE action = 'CPU';
```

# OPatch

- Use OPatch inventory to determine if CPU patch applied to ORACLE\_HOME
  - Does not indicate if *catcpu.sql* has been run for databases
  - Not the most friendly output

```
# cd $ORACLE_HOME/OPatch
```

```
# ./opatch lsinventory -detail
```

# Common CPU Patching Mistakes

1. CPU Forgotten Steps
2. Database Upgrades
3. ORACLE\_HOME vs. Database
4. ORACLE\_HOME and New Database

# #1 CPU Forgotten Steps

- CPU is two parts –
  1. OPatch to update files in the ORACLE\_HOME
  2. catcpu.sql to update database objects
- Some CPUs require additional manual steps –
  - January 2008 CPU requires all views to be recompiled due view/SQL compiler bugs in July 2007 CPU
- Query `SYS.REGISTRY$HISTORY` to verify CPU row is present
  - An indicator CPU patch was successfully applied

## #2 Database Upgrades

- Scenario
  - Latest CPU patch is applied (January 2009)
  - Upgrade database to new version or patchset (10.2.0.3 to 10.2.0.4)
- Do I have to reapply the latest CPU after the database upgrade?
  - Yes, you must apply 10.2.0.4 January 2009 patch

# Database Upgrades and CPU Patches

Database Version Upgrade Patch	Latest CPU Patch Included In Upgrade Patch
9.2.0.8	July 2006
10.1.0.5	October 2005
10.2.0.3	October 2006
10.2.0.4	April 2008
11.1.0.6	October 2007
11.1.0.7	January 2009

## #3 ORACLE\_HOME vs. Database

- Scenario
  - Latest CPU patch is applied (January 2009) to ORACLE\_HOME
  - Install a new database from the patched ORACLE\_HOME
- Do I have to run the *catcpu.sql* from the January 2009 CPU?
  - Yes, since some of the SQL statements in the *catcpu.sql* do not exist as files in the Oracle Home
  - *catcpu.sql* does perform some drops and grants

## #4 ORACLE\_HOME and New Database

- Scenario
  - Latest CPU patch is applied (January 2009) to ORACLE\_HOME
  - Install a new database from the patched ORACLE\_HOME using DBCA and a seeded database
- Do I have to run the *catcpu.sql* from the January 2009 CPU?
  - Yes, since the seeded database files are pre-loaded with packages and none of the vulnerable packages would be updated without running *catcpu.sql*

# References

- Oracle Critical Patch Update January 2010 Advisory, 12 January 2010, <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>
- Security Alerts and Critical Patch Updates - Frequently Asked Questions", 30 July 2007, Oracle Metalink Note ID 360470.1
- Oracle Database Server and Networking Patches for Microsoft Platforms, 11 April 2010, Oracle Metalink Note ID 161549.1
- How can I see if a Critical Patch Update is installed on the database, 18 May 2009, Oracle Metalink Note ID 352783.1
- Critical Patch Update January 2010 Availability Information for Oracle Database and Fusion Middleware Products, 12 January 2010, Oracle Metalink Note ID 967472.1
- Integrity Corporation, "An Introduction to SQL Injection Attacks for Oracle Developers", [http://www.integrity.com/security-resources/whitepapers/Integrity Oracle SQL Injection Attacks.pdf](http://www.integrity.com/security-resources/whitepapers/Integrity%20Oracle%20SQL%20Injection%20Attacks.pdf), March 2007

*Questions?*

# Contact Information

**Stephen Kost**  
**Chief Technology Officer**  
**Integrigy Corporation**

**e-mail: [skost@integrigy.com](mailto:skost@integrigy.com)**  
**blog: [integrigy.com/oracle-security-blog](http://integrigy.com/oracle-security-blog)**

**For information on -**

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

**[www.integrigy.com](http://www.integrigy.com)**