

Oracle Critical Patch Updates – Insight and Understanding

Stephen Kost
Integrigy Corporation
Session # 359

Introduction

- **Stephen Kost**

- Chief Technology Officer of Integrigy Corporation
- 14 years experience with Oracle technology as database administrator, architect, and application administrator
- Found more than 40 security bugs fixed in CPUs

- **Integrigy Corporation**

- Firm is dedicated to Oracle Security
- Services – Oracle Security Assessments
- Products – AppSentry and AppDefend

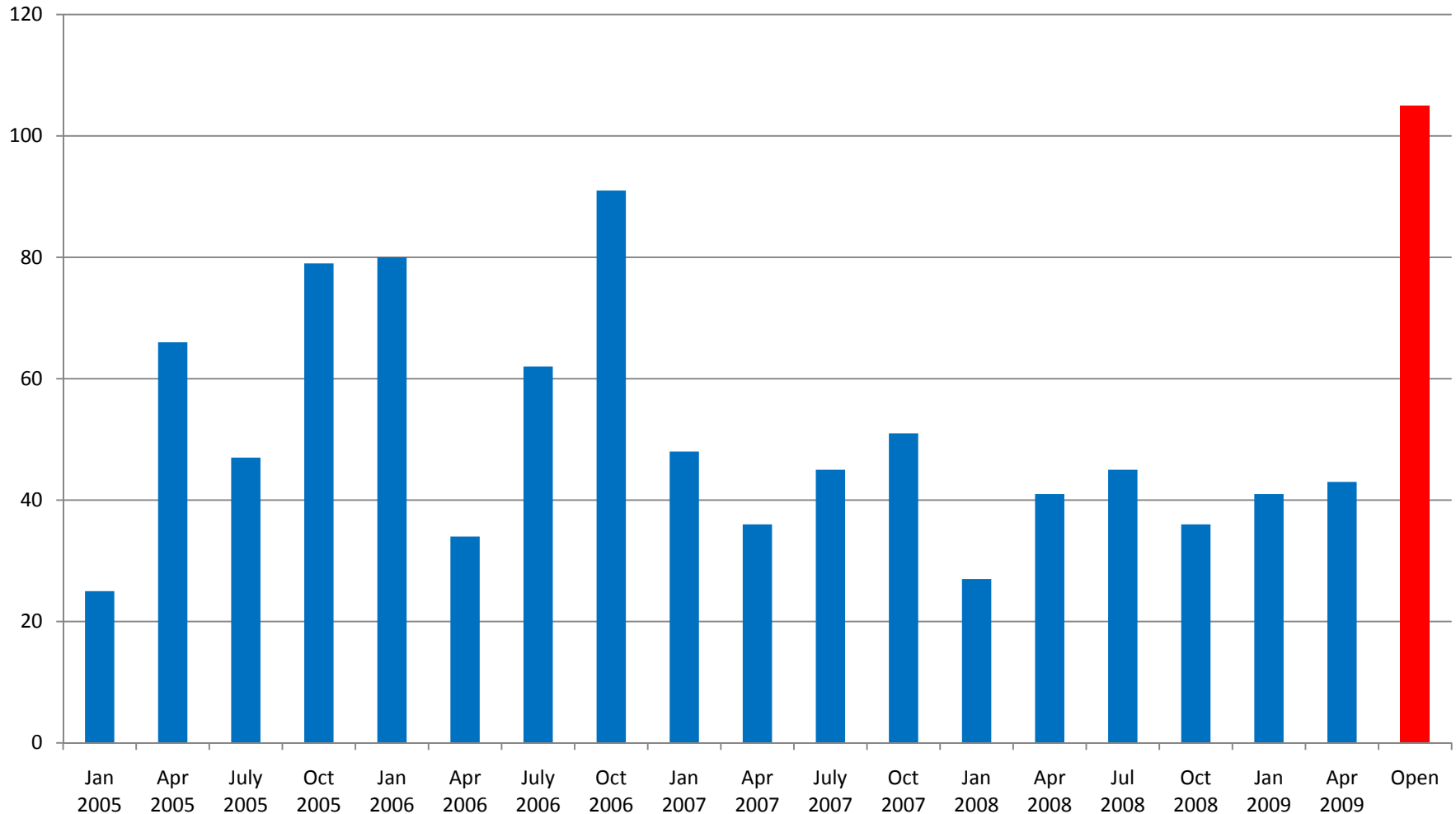
Agenda

- Background of Critical Patch Updates
- Vulnerabilities
- Certification vs. Certification
- Patches
- Patching Strategy
- Questions

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
 - Next CPUs = **July 14, 2009** and **October 13, 2009**
- **Eighteen** CPUs released to date starting with January 2005
 - 897 security bugs fixed (average is 50 bugs per CPU)
 - 374 bugs in the Oracle Database

Security Bugs per CPU (all products)



Security Bug Process



Bug reported

1. Customer or security researcher reports security bug to Oracle

2. Oracle researches bug and develops bug fix

– Finder not allowed to test fix or even notified about fix

3. Oracle may include fix in new releases

– No notification of security fixes to customers

4. Oracle includes fix in quarterly CPU

– **From initial report to security patch release is 3 months to 3 years**

Elapsed time on average is 18 months

Bug fixed

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 metric, not Oracle
- **Oracle Database realistic maximum is 5.5 to 6.5**
- **Oracle includes “Partial+” in the advisory**

Types of Oracle Security Bugs

- Buffer Overflow
- SQL Injection
- Parameter Tampering
- Permission Issues
- Information Disclosure

% of Bugs Exploitable with No Auth

4%

For the CPUs January 2007 through January 2009 (5 of 133 database bugs)

% of Bugs PUBLIC Exploitable

41%

For the CPUs January 2007 through January 2009 (54 of 133 database bugs)

% of Published Exploits PUBLIC Exploitable

87%

For the CPUs January 2007 through January 2009 (21 of 24 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 (January 2009)

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

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 Listener Invited Nodes feature

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 2009 Advisory, 13 January 2009, <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.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, 23 April 2007, Oracle Metalink Note ID 161549.1
- How can I see if a Critical Patch Update is installed on the database, 26 March 2009, Oracle Metalink Note ID 352783.1
- Critical Patch Update January 2009 Availability Information for Oracle Database and Fusion Middleware Products, 13 January 2009, Oracle Metalink Note ID 753340.1
- Integrity Corporation, "An Introduction to SQL Injection Attacks for Oracle Developers", http://www.integrity.com/security-resources/whitepapers/Integrity_Oracle_SQL_Injection_Attacks.pdf, March 2007

Questions?

My Next Session

OAUG

Critical Patch Updates Unwrapped – Oracle E-Business Suite

Wednesday, 9:45am to 9:30am

Room 304G

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: skost@integrigy.com
blog: 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