

Oracle Critical Patch Updates Unwrapped

Stephen Kost
Integrigy Corporation

Introduction

■ Stephen Kost

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

■ Integrigy Corporation

- Only firm that is dedicated to Oracle E-Business Suite Security
- Services – Oracle Applications Security Assessments
- Products – AppSentry and AppDefend

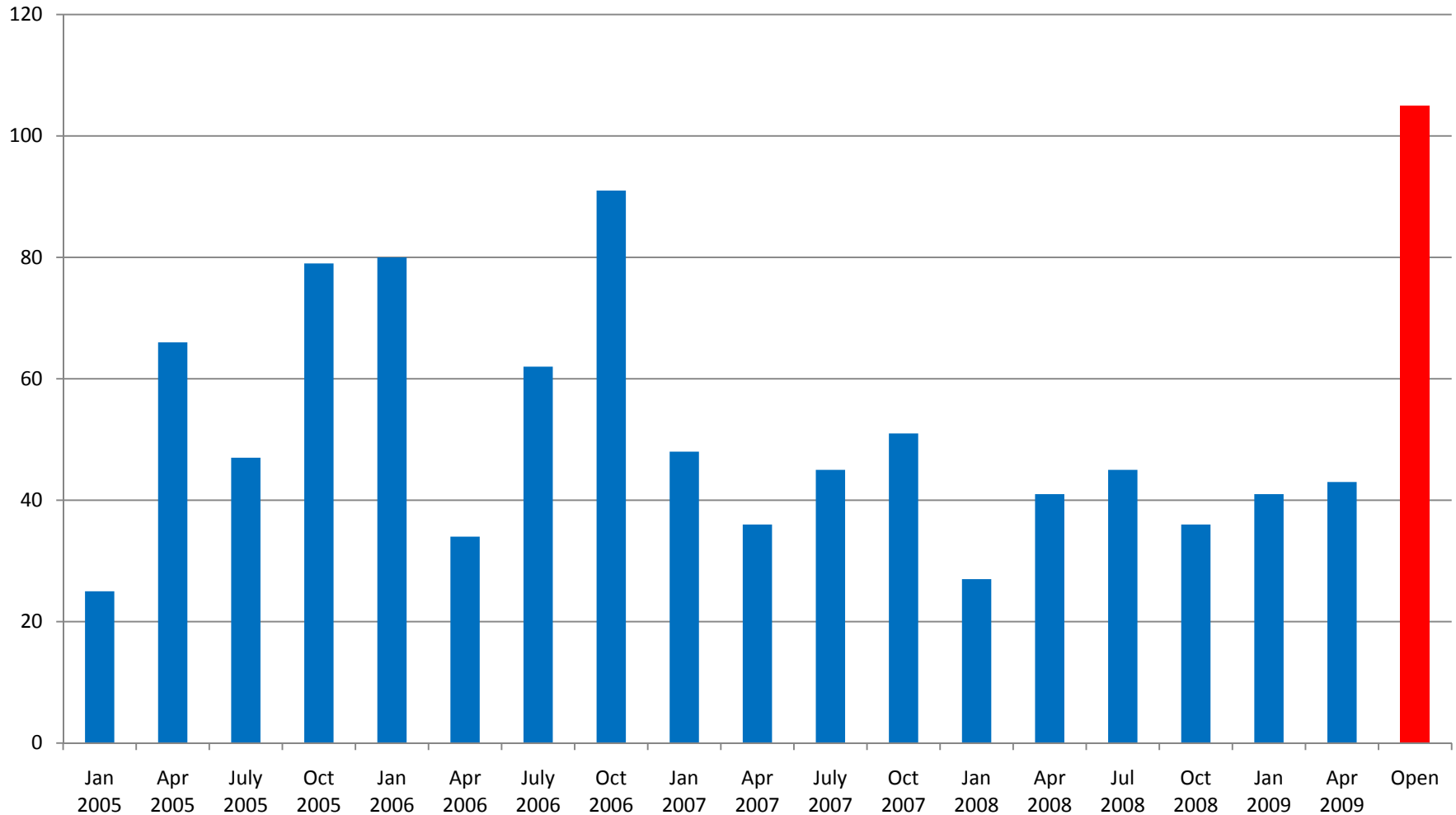
Agenda

- 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
 - 182 bugs in the Oracle E-Business Suite 11i and R12

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
- Cross-site Scripting (XSS)
- 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?

APPLSYS/PUB

and anyone else with a database account

Database Vulnerabilities (Jan09/11i)

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

Oracle Applications 11i Baseline

- Critical Patch Updates require an Oracle Applications 11i minimum ATG_PF.H RUP level
 - Starting in July 2007, must be RUP(n) or RUP(n-1)
 - RUP(n) or RUP(n-1) for all versions 11.5.9 through 11.5.10.2
 - **April 2009 requires RUP5 or RUP6**

Metalink Certification != CPU Certification

- Controlled by Oracle Software Error Correction Support Policy
- CPUs only certified with latest two patch sets released in the past 12 months

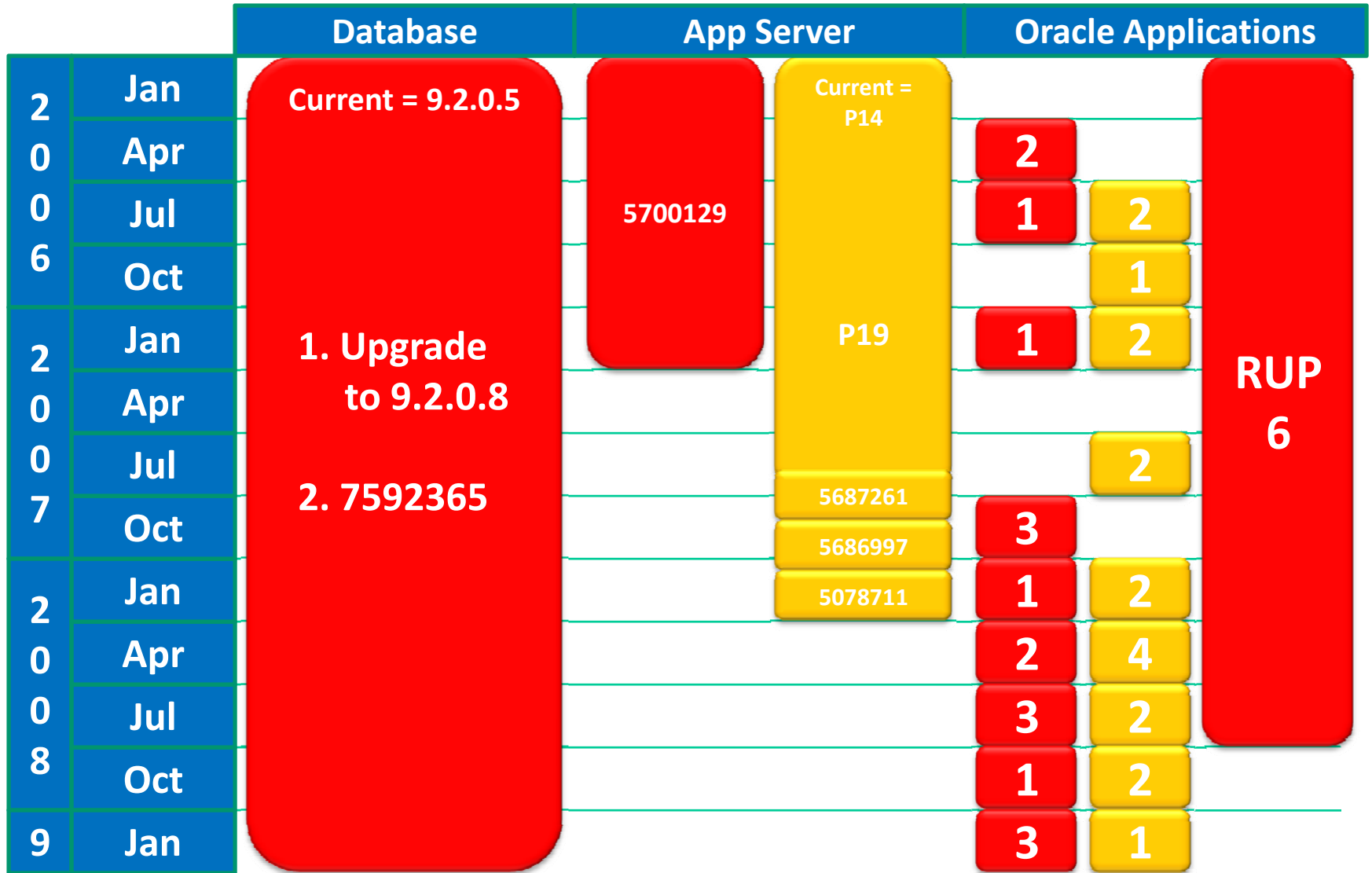
Apps Version	Database	App Server (Apache)	Developer	JInitiator (WinXP)	ATG_PF
11.5.10.2	9.2.0.4 – 7 9.2.0.8 10.1.0.4 10.1.0.5 10.2.0.2 – 3 10.2.0.4 11.1.0.6 – 7	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.24 (P15)* 6.0.8.x (P16 - P18) 6.0.8.27 (P19)	1.1.8.19–25 1.1.8.27 1.3.1.18* 1.3.1.21 - 28 1.3.1.29	ATG_PF.H* ATG_PF.H RUP5 or ATG_PF.H RUP6

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 Applications Patches (Jan09)

Patches	Scope/ Risk	Patch Complexity	Vulnerability Description and Testing
7567354	Medium	Low	<p>Application Object Library (FND)</p> <ul style="list-style-type: none"> Authentication is added to old-style personal home pages to prevent users from renaming, deleting, etc. other user's pages. Review the Apache access logs to determine if the web page "OracleConfigure" is being accessed. If it is accessed, be sure to test this page. Otherwise, no testing is required. Mandatory for all implementations, especially those still using old-style personal home pages. All these pages are blocked by the URL Firewall for external access.
7610955	Medium	Medium	<p>iProcurement</p> <ul style="list-style-type: none"> Security vulnerabilities in the iProcurement shopping and search results web pages. A regression test of iProcurement shopping, searching, and requisition web pages should be performed as there are a number of dependent pages that may be updated. Mandatory for all implementations. All these pages are by default blocked by the URL Firewall for external access.



Patching Strategy

- General advice –
 - Apply the Database patch – cumulative for all CPUs and previous security alerts
 - Apply Oracle Applications patches – not cumulative, must apply all patches from all previous CPUs
 - Evaluate the effort to apply Developer 6i, Application Server, and JInitiator patches – depending on risk and effort, delaying these patches may be warranted
- Specific advice –
 - Integrity releases guidance for each CPU on our website
 - Each CPU has unique issues and requirements, thus need to be evaluated independently

References

- Integrigy, “Oracle Critical Patch Update January 2009 E-Business Suite Impact”, www.integrigy.com
- Integrigy, “Oracle Jinitiator 1.1.8 Buffer Overflow Vulnerability Analysis”, www.integrigy.com
- Oracle, “Oracle Critical Patch Update January 2009 Advisory”, <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Oracle Corporation, “Oracle E-Business Suite Critical Patch Update Note January 2009”, Metalink Note ID [738923.1](#)
- Oracle Corporation, “Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10”, Metalink Note ID [363827.1](#)
- Oracle Corporation, “Database, FMW, and OCS Software Error Correction Support Policy Version 2.1”, Metalink Note ID [209768.1](#)

Questions?

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