

Oracle Critical Patch Update

July 2011

E-Business Suite Impact

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

July 28, 2011



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

Background

Speaker

Stephen Kost

- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, ...

Company

Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

Integrigy Security Alerts

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

Agenda

Background of
Oracle CPUs

Patches

Q&A



Vulnerabilities

Patching
Strategy

Agenda

Background of
Oracle CPUs

Patches

Q&A

1

2

3

4

5

Vulnerabilities

Patching
Strategy

Oracle Critical Patch Updates

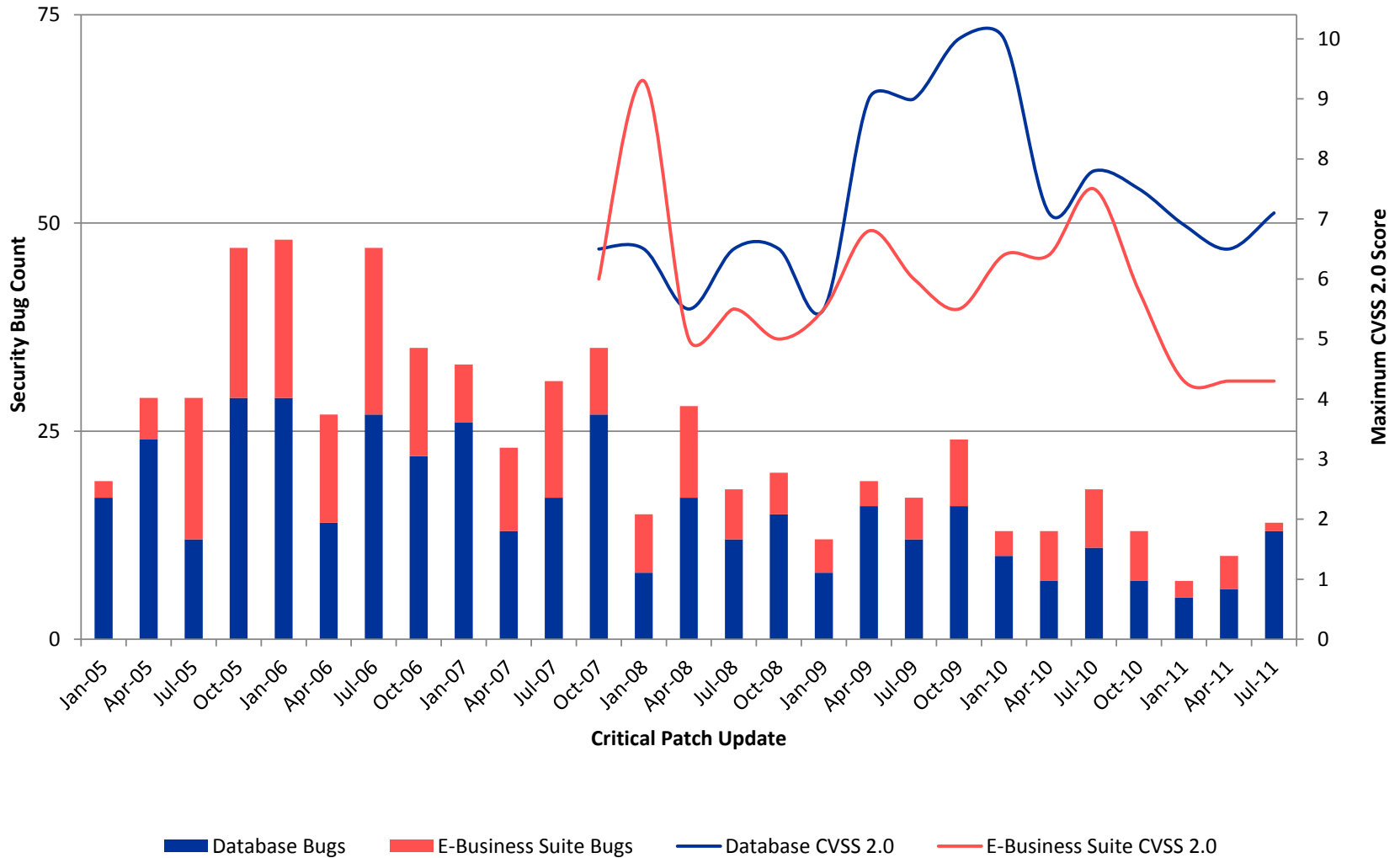
Fixes for security bugs in all Oracle products

- Released quarterly on a fixed schedule
- Tuesday closest to the **17th** day of January, April, July and October
- Next CPUs = **October 18, 2011** and **January 17, 2012**

Twenty-seven CPUs released to date starting with January 2005

- 1,301 security bugs fixed (average is 48 bugs per CPU)
- 420 bugs in the Oracle Database
- 224 bugs in the Oracle E-Business Suite

Oracle Security Bugs per Quarter



CPU Recent Changes

- **Oracle E-Business Suite 11i Cumulative Patches**
 - Introduced with January 2010 CPU
 - Supports 11.5.10 CU2 only
 - **January 2011 and onward only Cumulative Patches**
- **Oracle CPU High-level Summary**
 - New text form summary of the CPU content
 - No new information
 - Limited value

Oracle Security Bug Process



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 first 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**

Oracle and CVSS

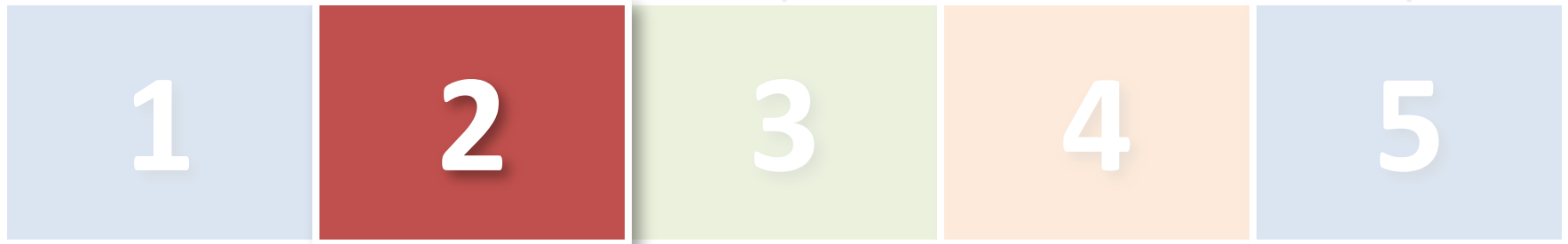
- **CVSS = Common Vulnerability Scoring System**
 - A common scoring for the risk and severity of vulnerabilities - base metric score is 1 to 10 (10=worst)
 - Designed for network devices and servers, not databases and applications – biased toward root access
- ***Oracle CVSS base metric scores will 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**

Agenda

Background of
Oracle CPUs

Patches

Q&A



Vulnerabilities

Patching
Strategy

Oracle Database Vulnerabilities (July 2011)

CVE	Component	Notes
CVE-2011-2239 CVE-2011-2253	Core RDBMS	<ul style="list-style-type: none"> ▪ Buffer overflows in libraries? ▪ Requires CREATE LIBRARY or SYSDBA ▪ Fully compromise Windows server – maybe limited on Unix/Linux
CVE-2011-0835 CVE-2011-0880 CVE-2011-0838 CVE-2011-0832	Core RDBMS	<ul style="list-style-type: none"> ▪ DBMS_HS_PARALLEL and DBMS_HS_PARALLEL_METADATA Packages ▪ Only CREATE SESSION required ▪ 11gR1 and 11gR2 only
CVE-2011-2232 CVE-2011-2231	XML Developers Kit	<ul style="list-style-type: none"> ▪ XML Developers Kit – XML Processing Security Bug ▪ Authenticated session ▪ libxml is patched
CVE-2011-2230	Core RDBMS	<ul style="list-style-type: none"> ▪ Denial of Service (DoS) in core database ▪ Remotely exploitable without authentication ▪ Different than previous DoS vulnerabilities in Listener

Oracle Database Vulnerabilities (July 2011)

CVE	Component	Notes
CVE-2011-2238	Database Vault	<ul style="list-style-type: none">▪ Database Vault Privilege Escalation Issue▪ Required EXECUTE on DBMS_SYS_SQL
CVE-2011-2243	Core RDBMS	<ul style="list-style-type: none">▪ Create session and trigger as SYSDBA▪ 11gR1 and 11gR2 only▪ Probably a buffer overflow
CVE-2011-2240	Oracle Universal Installer	<ul style="list-style-type: none">▪ Access to local file system only▪ 10.1.0.5 only▪ Probably sensitive information in log files▪ Separate patch for OUI
CVE-2011-2242	Core RDBMS	<ul style="list-style-type: none">▪ XML DB FTP Server Local Access Issue▪ 11gR1 and 11gR2 only▪ Local account and Database account with privilege to login to XML DB FTP

Agenda

Background of
Oracle CPUs

Patches

Q&A



1

2

3

4

5

Vulnerabilities

Patching
Strategy

Critical Patch Updates Baselines

Database Version Upgrade Patch	Included CPU
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011

EBS Version	Included CPU
12.0.6	October 2008
12.1.1	April 2009
12.1.2	October 2009
12.1.3	January 2011

At time of release, usually the latest available CPU is included

Database CPU Support

Database Version	Terminal CPU
10.1.0.5	January 2012 (b)
10.2.0.4	July 2011 (a)
10.2.0.5	July 2013 (b)
11.1.0.7	July 2015 (b)
11.2.0.1	July 2011 (a)
11.2.0.2	July 2013 (est.) (a)

(a) Oracle CPU Support Date (b) Oracle Lifetime Support Date
(est.) Date estimated by Integrigy

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 patchset upgrade (i.e., 10.2.0.3 to 10.2.0.4)
 - Some Integrigy 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

- **July 2011 for 11.2.0.2 – Bug Fixes**
 - CPU = 15
 - PSU = 110
- **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

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';
```

Oracle Application Server Patches (July 2011)

	11.5.10.2	12.0.x	12.1.x
10.1.3.5		July 2011	July 2011
10.1.3.4		January 2010	January 2010
10.1.3.3		July 2009	July 2009
10.1.2.3		July 2011	July 2011
10.1.2.2		January 2009	January 2009
9iAS 1.0.2.2.2	January 2007		
Developer 6i	October 2008		

Oracle E-Business Suite CPU Baseline

- **Oracle E-Business Suite 11.5.10.x**
 - **Requires Extended Support Baseline (Metalink 883202.1)**
 - Equivalent to 11.5.10 CU2 + additional patches
 - July 2011 requires RUP6 or RUP7
- **Oracle E-Business Suite 12.0**
 - July 2011 requires 12.0.4
 - July 2011 requires ATG 12.0.6 (R12.ATG_PF.A.Delta.6)
- **Oracle E-Business Suite 12.1**
 - July 2011 requires 12.1.1

Oracle E-Business Suite 11i Cumulative

- Introduced with January 2010 CPU
- **July 2011 CPU Only Cumulative Patches**
- **Specific patches for ATG RUP 6 and RUP 7**
- **Almost Cumulative**
 - A number pre and post patches required for specific modules – see patch README
 - A few one-off CPU patches

Oracle E-Business Suite Vulnerabilities (July 2011)

CVE	Importance	Fix Complexity	Notes
CVE-2011-2246	Medium	Low	Business Intelligence <ul style="list-style-type: none">▪ biserror.jsp last updated for 11i in September 2006▪ Remotely exploitable without authentication▪ No testing required▪ Recommended for all implementations▪ This page is blocked by the URL firewall for external access

Agenda

Background of
Oracle CPUs

Patches

Q&A

1

2

3

4

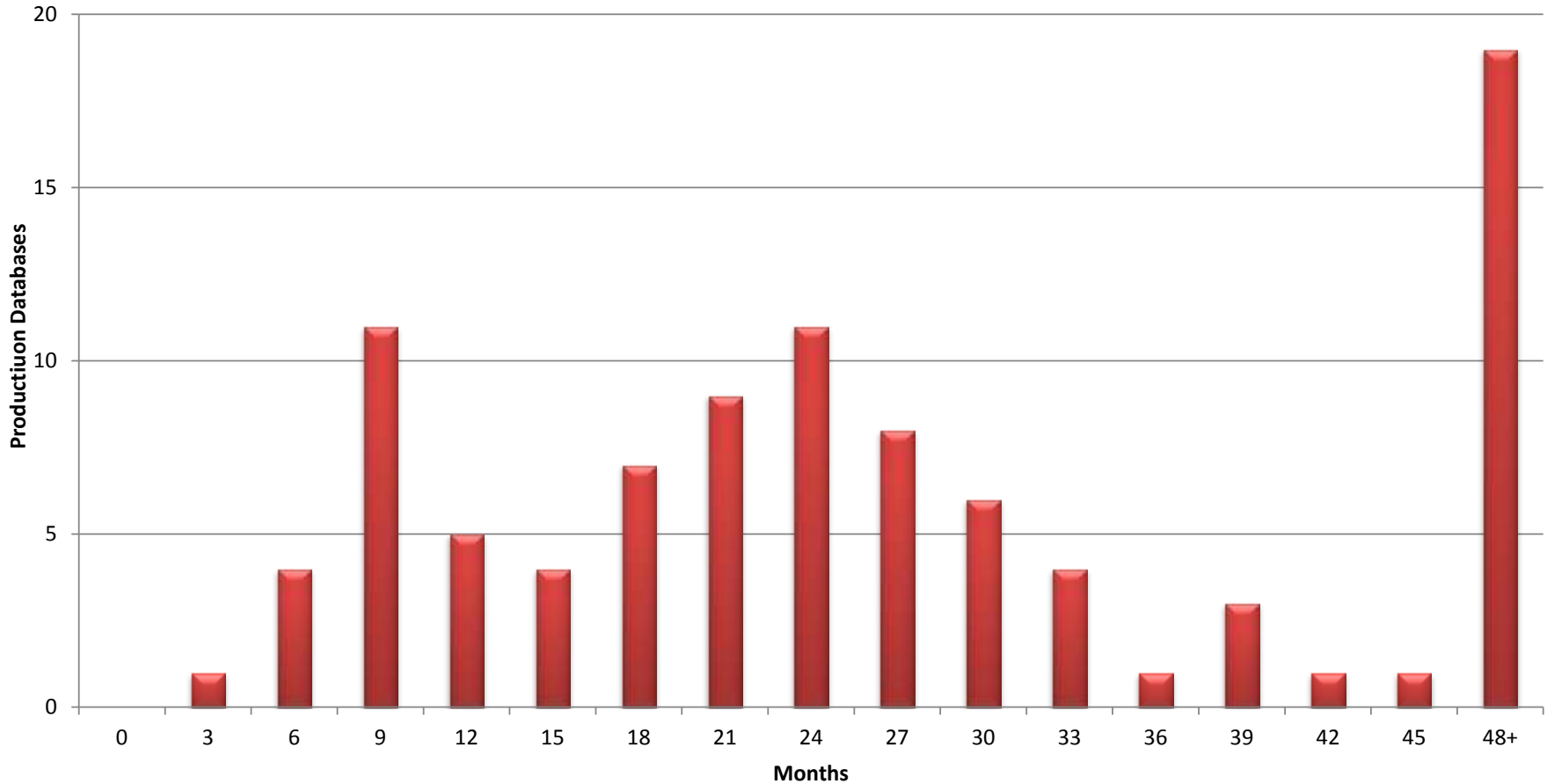
5

Vulnerabilities

Patching
Strategy

Oracle CPU Patching Metric

Security Patches - Months Behind



Patching Strategy

- **General advice –**

- Apply the Database patch – cumulative for all CPUs and previous security alerts
- Apply Oracle E-Business Suite patches – evaluate July 2011 cumulative patch
- Evaluate the effort to apply Developer and Application Server – depending on risk and effort, delaying these patches may be warranted

- **Specific advice –**

- Integrigy releases guidance for each CPU on our website
- Each CPU has unique issues and requirements, thus need to be evaluated independently

Agenda

Background of
Oracle CPUs

Patches

Q&A



Vulnerabilities

Patching
Strategy

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

For more information, www.integrigy.com

e-mail: info@integrigy.com

blog: integrigy.com/oracle-security-blog

Upcoming Integrigy Webinars

Oracle Critical Patch Update July 2011

Oracle Database Impact

- **Tuesday, August 2nd 2pm EDT**