INTEGRIGY

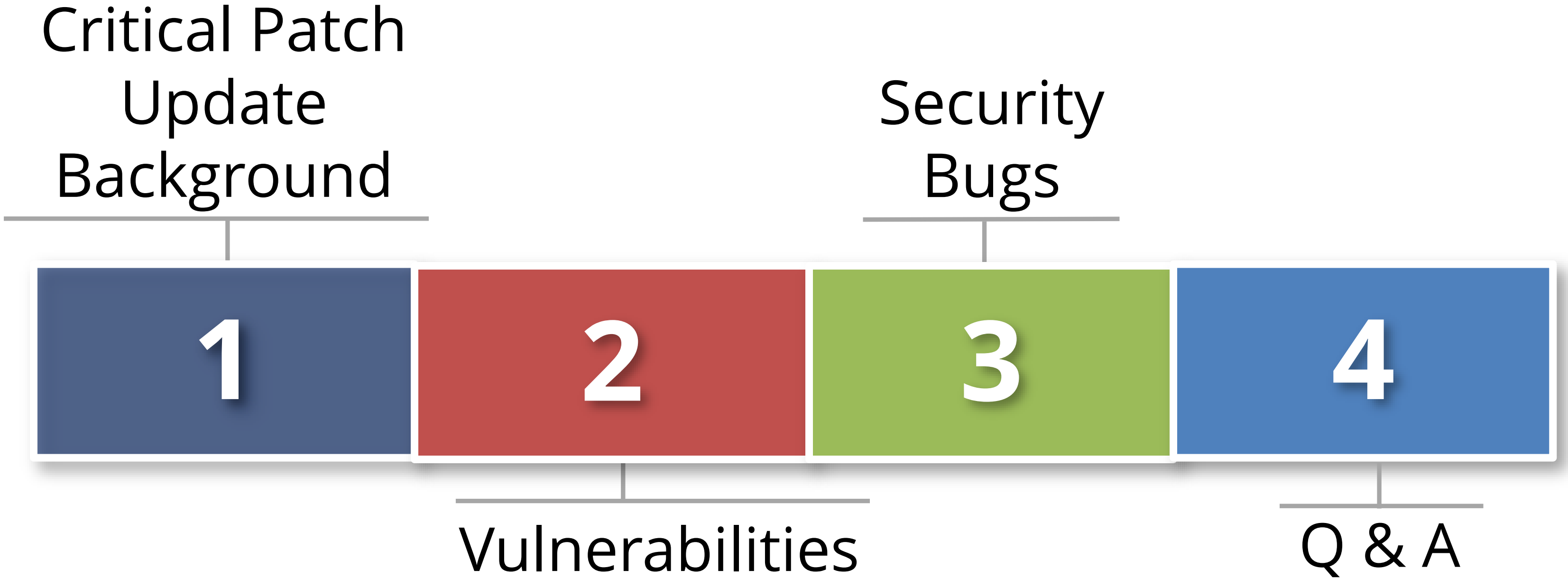
Security Boot Camp
Oracle Database Security Vulnerabilities Explained

May 22, 2012

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



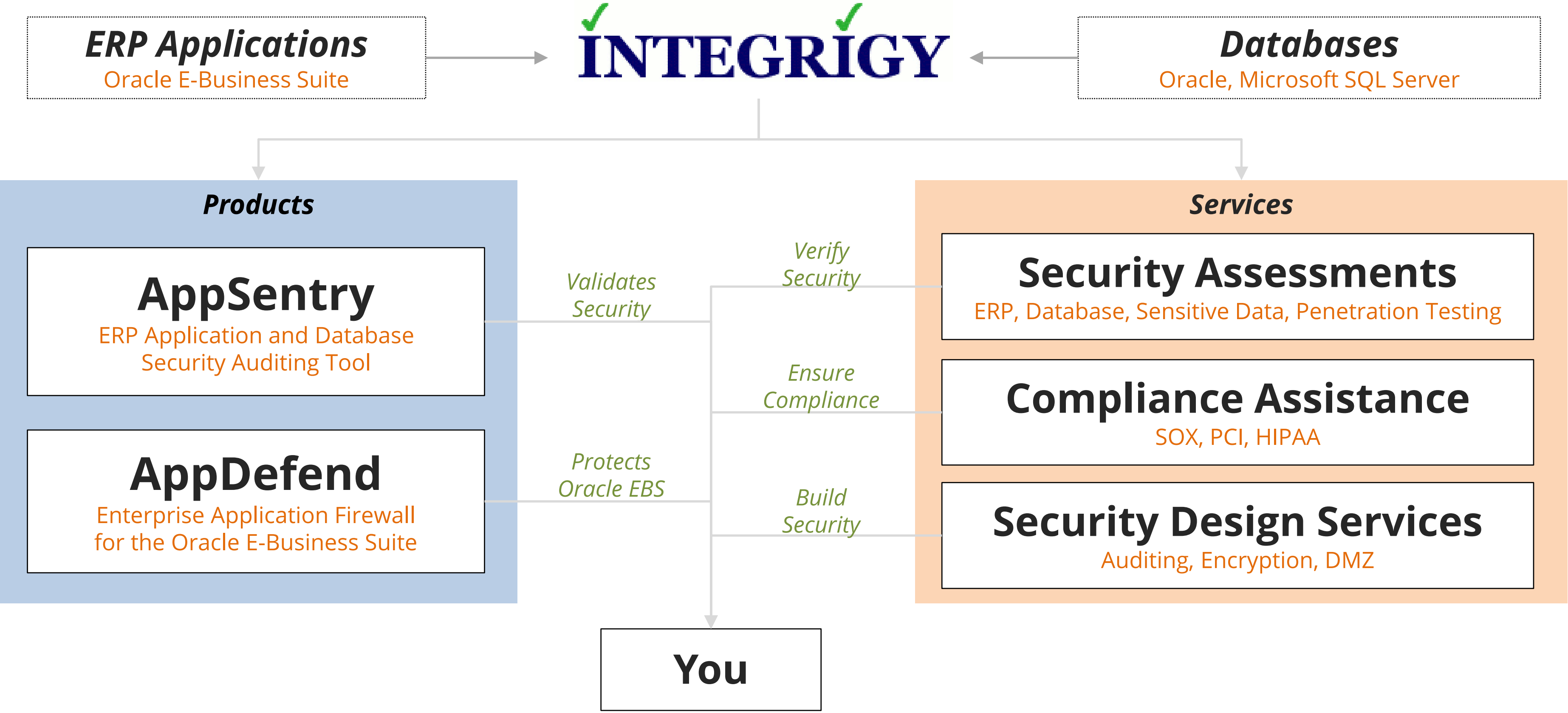
1 Critical Patch Update Background

2 Vulnerabilities

3 Security Bugs

4 Q & A

About Integrigy



ERP Applications

Oracle E-Business Suite

INTEGRIGY

Databases

Oracle, Microsoft SQL Server

Products

AppSentry

ERP Application and Database Security Auditing Tool

AppDefend

Enterprise Application Firewall for the Oracle E-Business Suite

Services

Security Assessments

ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance

SOX, PCI, HIPAA

Security Design Services

Auditing, Encryption, DMZ

Validates Security

Protects Oracle EBS

Verify Security

Ensure Compliance

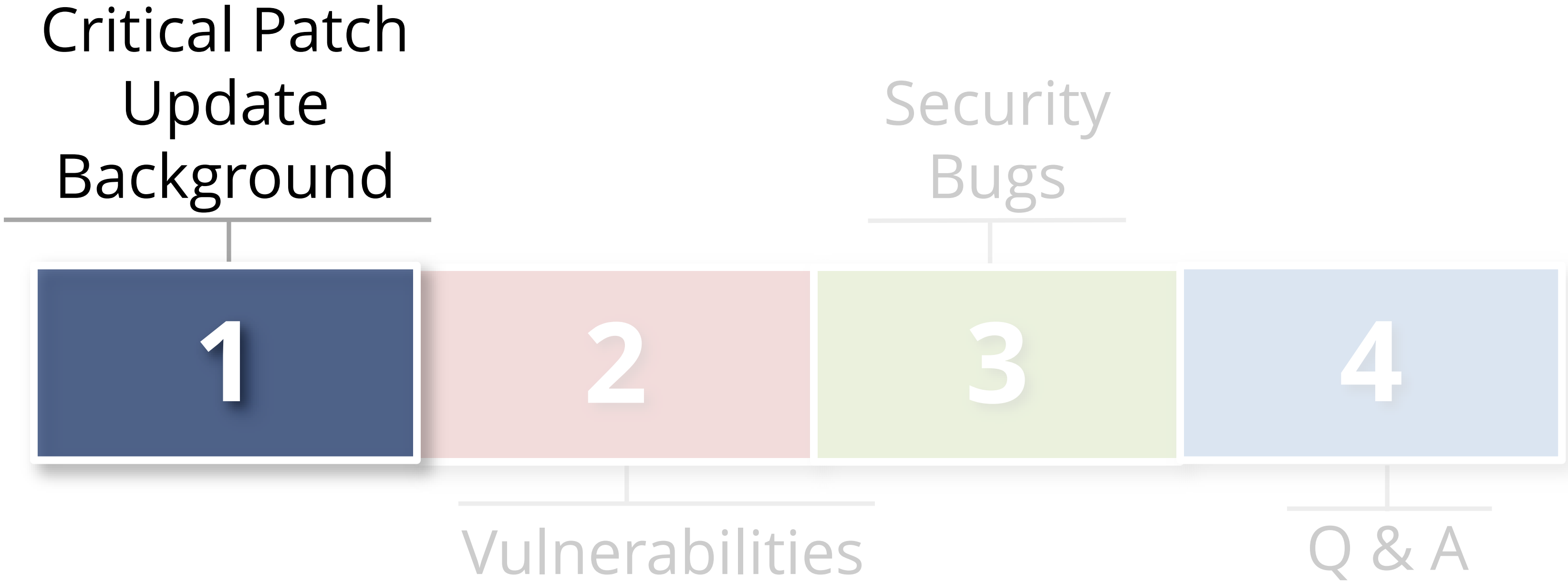
Build Security

You

Integrigy Published Security Alerts

Security Alert	*Versions*	*Security Vulnerabilities*
Critical Patch Update April 2012	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security architecture issue
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 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	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities and Information disclosure
Critical Patch Update April 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities and Information disclosure
Critical Patch Update Jan 2005	11.0.x, 11.5.1 – 11.5.10	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ 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	▪ No authentication in FNDFS program ▪ Retrieve any file from O/S

Agenda



1 Critical Patch Update Background

2 Vulnerabilities

3 Security Bugs

4 Q & A

Oracle Critical Patch Updates

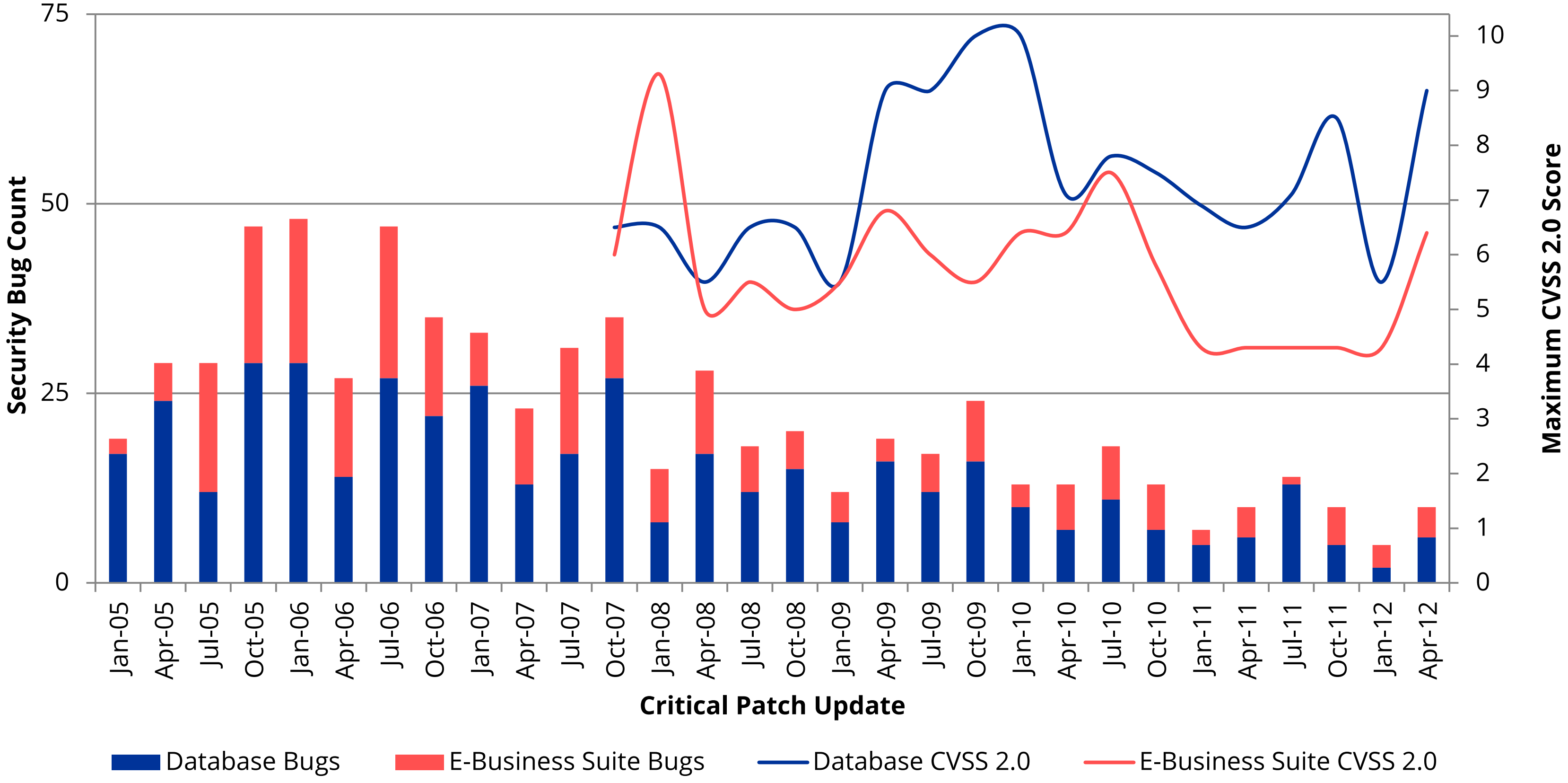
Fixes for security bugs in all Oracle products

- Released quarterly on a fixed schedule
- Tuesday closest to the **17th** day of January, April, July and October
- Next CPUs = **July 17, 2012** and **October 16, 2012**

Thirty CPUs released to date starting with January 2005

- **1,379** security bugs fixed (average is 47 bugs per CPU)
- **433** bugs in the Oracle Database
- **236** bugs in the Oracle E-Business Suite

Oracle Security Bugs per Quarter



Oracle Security Bug Process

Bug reported

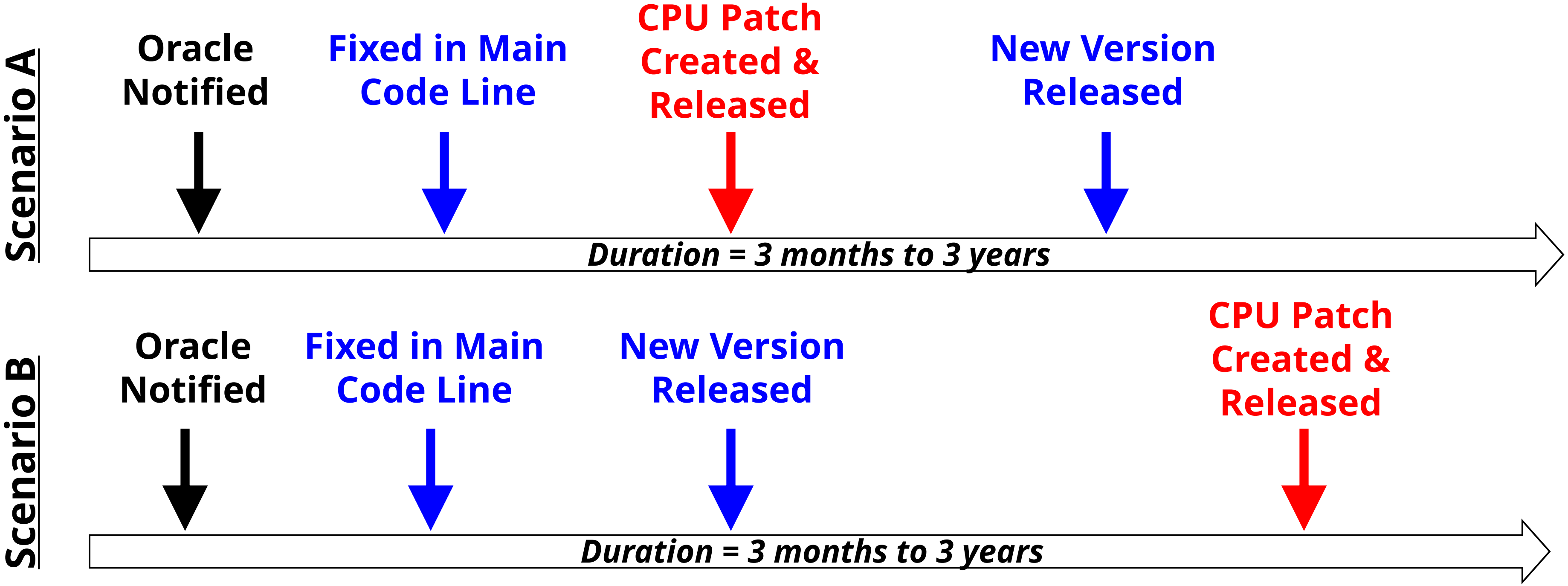
Elapsed time on average is 18 months

Bug fixed

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 Security Bug Process

Vulnerability may be fixed first in a new version (e.g., 11.2.0.2) before through a Critical Patch Update with no notification



Scenario A

Oracle Notified

Fixed in Main Code Line

CPU Patch Created & Released

New Version Released

Duration = 3 months to 3 years

Scenario B

Oracle Notified

Fixed in Main Code Line

New Version Released

CPU Patch Created & Released

Duration = 3 months to 3 years

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
11.2.0.3	July 2011

At time of release, usually the latest <u>available</u> CPU is included

Database CPU Support

Database Version	Terminal CPU
10.1.0.5	January 2012 (b)
10.2.0.4	July 2011 (a)(c)
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	January 2013 (a)
11.2.0.3	July 2014 (d)

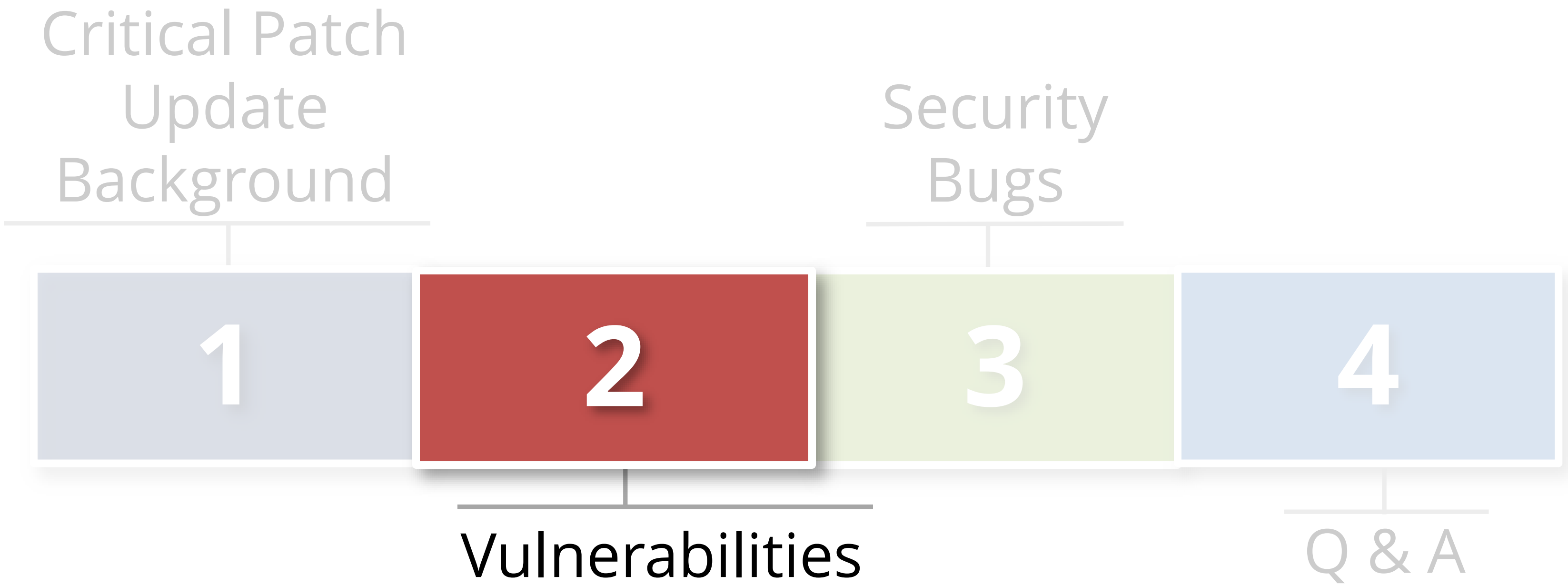
(a) Oracle CPU Support Date

(c) Supported only on limited platforms

(b) Oracle Lifetime Support Date

(d) Estimated by Integrigy

Agenda



1 Critical Patch Update Background

2 Vulnerabilities

3 Security Bugs

4 Q & A

Oracle Database Vulnerability Breakdown

~40%	SQL Injection
~20%	Buffer Overflow
~10%	Privilege or Permission Issue
~30%	Other

Total Vulnerabilities = 433

% of Bugs Exploitable with No Auth

19%

For the CPUs January 2007 through January 2012 (47 of 253 database bugs)

% of Bugs PUBLIC Exploitable

53%

For the CPUs January 2007 through January 2012 (133 of 253 database bugs)

% of Published Exploits PUBLIC Exploitable

44%

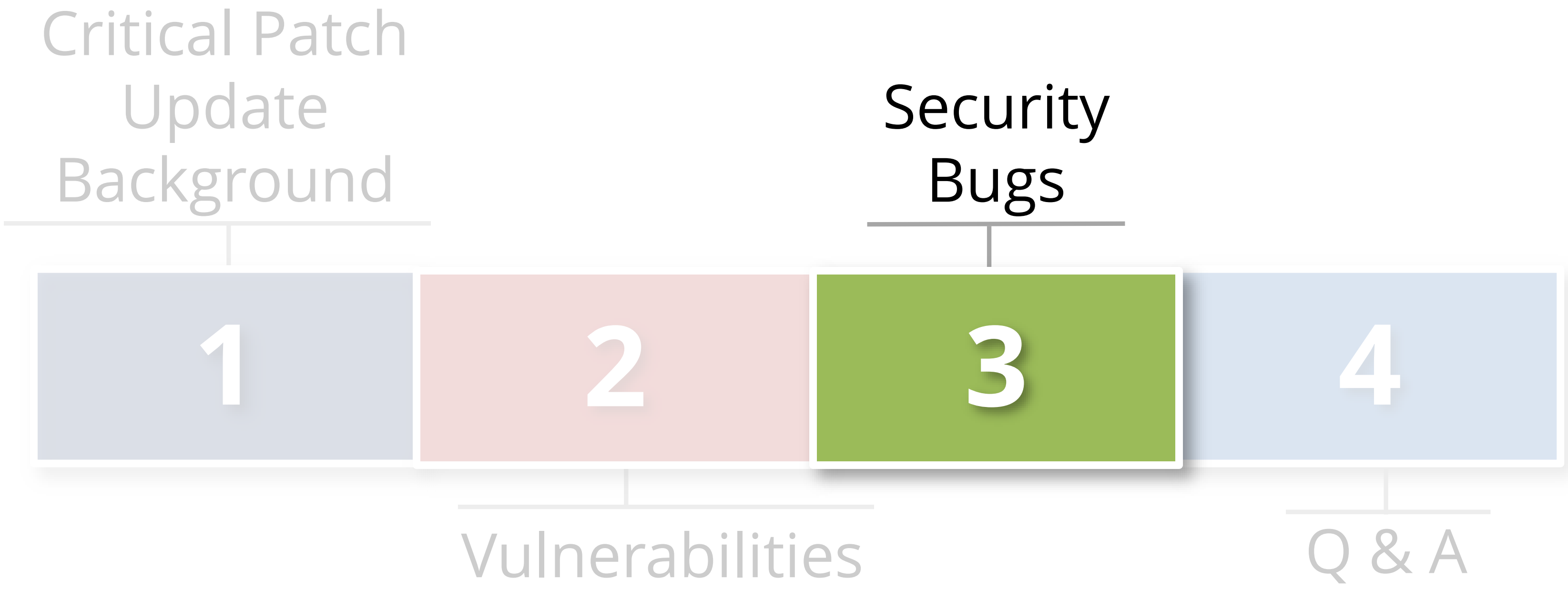
For the CPUs January 2007 through January 2012 (59 of 133 database bugs)

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

Agenda



Critical Patch Update Background

1

2

Vulnerabilities

Security Bugs

3

4

Q & A

Oracle Security Bug Walkthrough

- **SQL Injection**

  January 2009 – MDSYS.SDO_TOPO_DROP_FTBL Trigger (CVE-2008-3979)

- **Privilege Issue**

  April 2010 – Java Public Privilege on DBMS_JVM_EXP_PERMS (CVE-2010-0867)

- **Design Flaw**

  January 2012 – Oracle SCN Escalation (CVE-2012-0082)

SQL Injection – SDO_TOPO_DROP_FTBL

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2008-3979	Oracle Spatial	Oracle Net	Drop Table, Create Procedure	No

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.5	Network	Low	Single	Partial+	Partial+	None	10.1.0.5, 10.2.0.2

Privilege Issue – DBMS_JVM_EXP_PERMS

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2010-0867	Java VM	Oracle Net	Create Session	No

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
4.0	Network	Low	Single	None	Partial+	None	10.2.0.4, 11.1.0.7, 11.2.0.1.0

Design Flaw – Oracle SCN

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-0082	Core RDBMS	Oracle Net	Create Session	No

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.5	Network	Low	Single	None	Partial	Partial+	10.1.0.5, 10.2.0.5, 11.1.0.7, 11.2.0.3

Oracle Database SCN

System Change Number (SCN)

A database ordering primitive. The value of an SCN is the logical point in time at which changes are made to a database.

- **Internal Timestamp**

  SCNs order events within the database, which is necessary for redo and read consistency

- **281 Trillion Limit**

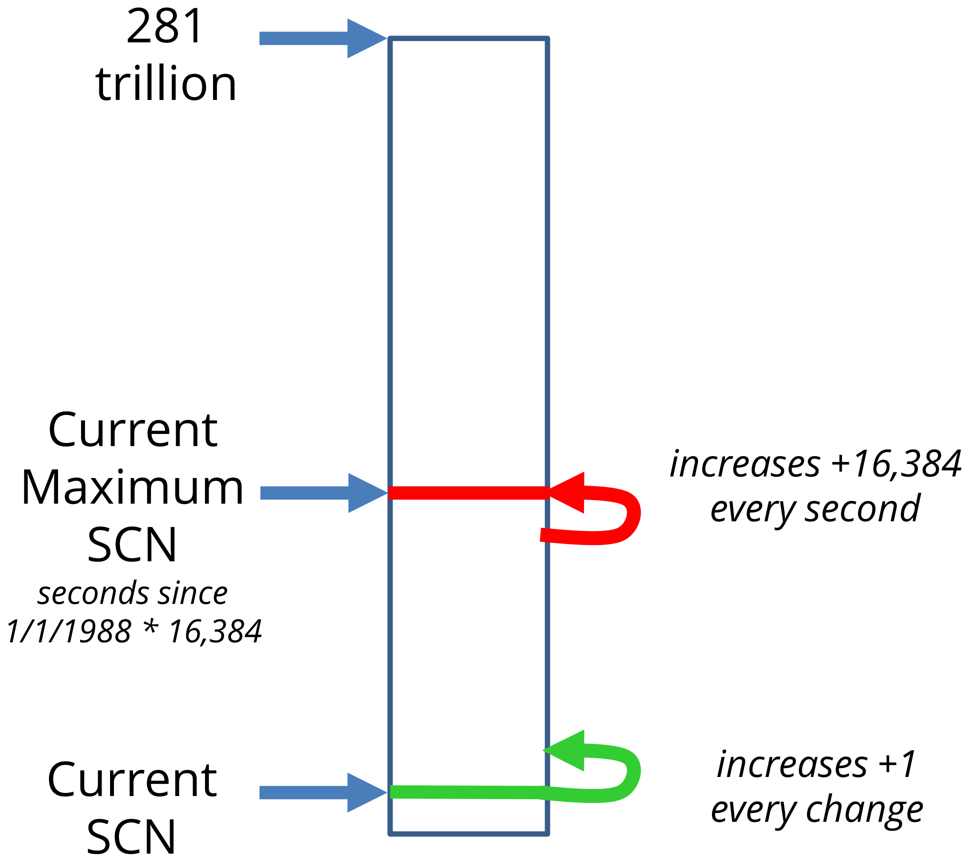
  48-bit number – 500 year limit – *immaterial for this discussion*

- **Current Maximum SCN**

  Database cannot exceed “time-based rationing system” for SCNs which is recalculated every second = seconds since 1988 * 16384

  ORA-600 errors occur if the Current Maximum SCN is exceeded

SCN Illustrated


281 trillion
Current Maximum SCN
*seconds since 1/1/1988 * 16,384*
increases +16,384 every second
Current SCN
increases +1 every change

- 281 trillion upper limit will not be reached for 500 years – this limit really doesn't matter
- **Current Maximum SCN** increases +16,384 every second
- **Current SCN** increases +1 with most changes
- Current SCN cannot exceed Current Maximum SCN – otherwise ORA-600 [2252] for any changes

SCN Increments

1 Each database change

- Transaction commits
- Transactions within same second may have same SCN

2 Distributed transactions – database links

- Synchronizes local and remote databases to highest SCN

3 Software bugs

- ALTER DATABASE BEGIN BACKUP – doesn’t turn off
- *How many more issues exist?*

“However, Oracle has determined that ***some software bugs*** *could cause the database to exceed the current maximum SCN value.”*

*“****All*** *the associated bugs have been fixed in the January 2012 CPU (and associated PSU).”*

Oracle Bulletin, 17 January 2012

Design Flaw vs. Software Bug

Known software bugs are fixed in the January 2012 Critical Patch Update

Any new bugs still can cause errors when the current maximum SCN is exceeded

“But with steadfast consistency, Oracle has characterized the risk posed by these problems as ***minimal****. “*

InfoWorld, January 23, 2012

January 2012 Critical Patch Update

1 Known SCN escalation bugs fixed

- ALTER DATABASE BEGIN BACKUP fixed
- One or more other bugs fixed

2 Database Link SCN Sanity Check

- Database links from remote databases where the remote SCN is within <x> of the Current Maximum SCN will be rejected
- Hidden parameter **_external_scn_rejection_threshold_hours** added for 10g and 11.1 with a default of 24 hours

SCN Flaw State after Jan 2012 CPU

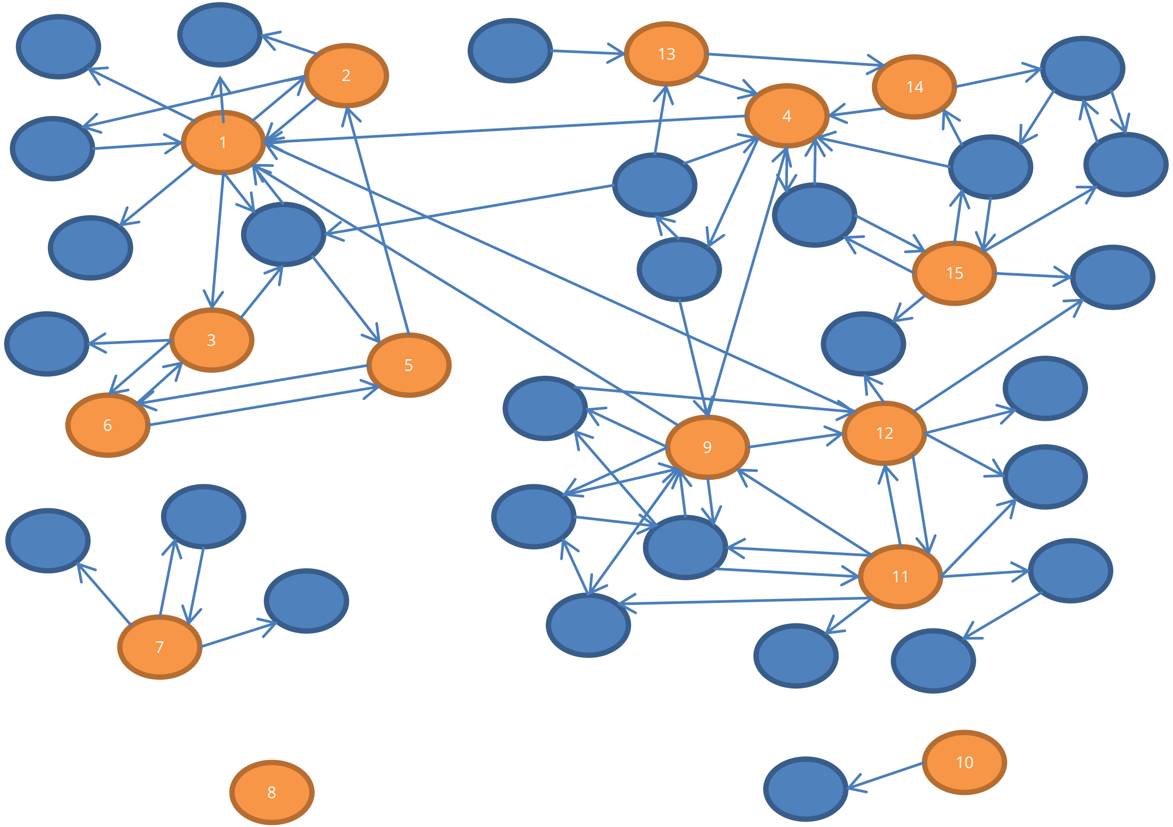
1 Fundamental flaw will always exist

- January 2012 CPU fixes bugs, but not the fundamental flaw
- It is still possible to stop database processing if SCN can be made to exceed Current Maximum SCN

2 Database link risk still exists

- Window of exceeding the Current Maximum SCN has been minimized to a few hours
- Worst-case scenario is database will be unavailable for several hours
- Must have a window for SCNs due to time zone differences and clock discrepancies

Database Link Case Study



Overview

- Organization with about 150 production Oracle Databases
- Integrigy assessed 15 key SOX and PCI compliance Oracle databases
- Reviewed database links for connectivity and appropriateness

Conclusion

Database links are widely used in most organizations

Example SCN Current State

Current Maximum SCN = 12,691,246,776,320

Instance	Version	Current SCN
Database A	10.2.0.5	8,399,825,495,842
Database B	10.1.0.4	5,965,078,978,284
Database C	10.2.0.4	8,399,825,745,153
Database D	10.2.0.4	8,399,826,124,718
Database E	9.2.0.7	8,399,825,011,234
Database F	10.2.0.4	8,399,826,360,924

Risk: Single Database

1 Limited risk to a single database

- Difficult to escalate the SCN beyond the Current Maximum SCN without DBA privileges - must set init parameters and bounce database
- Possible to crash a database with a directed attack (google: gokan atil scn)

2 Databases near Current Maximum SCN most at risk

- It is possible to increase the SCN rate per second with low overhead transactions, but to exceed a rate of 16,384 per second is difficult
- Must sustain for a long period to catch up to Current Maximum SCN

Risk: Interconnected Databases

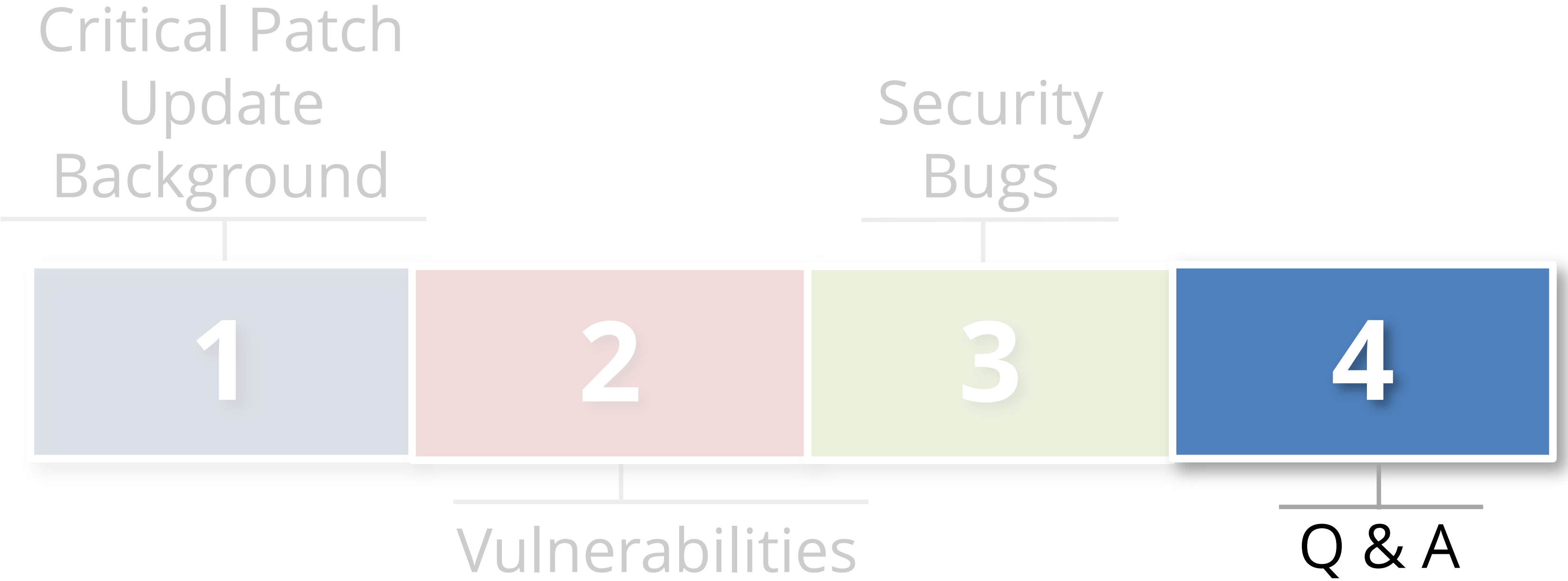
1 Accidental risk is low

- Requires a triggering event (such as ALTER DATABASE BACKUP bug) for escalated SCN rate on a high transaction volume database
- Will cascade through all interconnected databases

2 Malicious attack is feasible, but practical?

- Only requires access to a database account with CREATE SESSION on at least one database
- January 2012 CPU reduce possible impact
- No known attack methods that would require databases to be rebuilt (export/import)

Agenda



1 Critical Patch Update Background

2 Vulnerabilities

3 Security Bugs

4 Q & A

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**