mission critical applications …
… mission critical security

Oracle Critical Patch Update
October 2011
Oracle Database Impact

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

November 3, 2011

INTEGRIGY

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

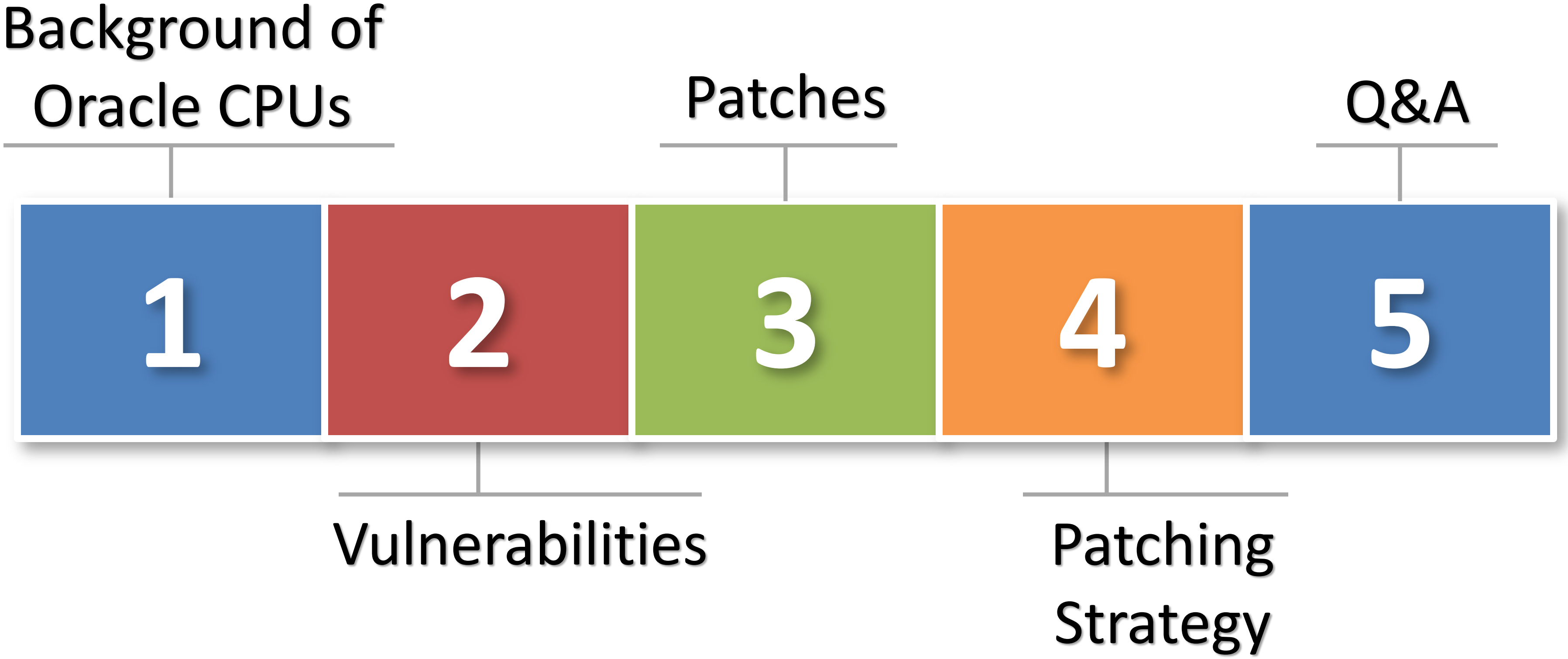
- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update July 2008	**Oracle 11g 11.5.8 – 12.0.x**	▪ 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	**11.5.1 – 11.5.10 11.0.x**	▪ Default configuration issues
Critical Patch Update July 2005	**11.5.1 – 11.5.10 11.0.x**	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update April 2005	**11.5.1 – 11.5.10 11.0.x**	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update Jan 2005	**11.5.1 – 11.5.10 11.0.x**	▪ SQL injection vulnerabilities
Oracle Security Alert #68	**Oracle 8i, 9i, 10g**	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	**11.5.1 – 11.5.8 11.0.x**	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	**11.5.1 – 11.5.8 11.0.x**	▪ 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

INTEGRIGY

Agenda



Background of Oracle CPUs

Patches

Q&A

1

2

3

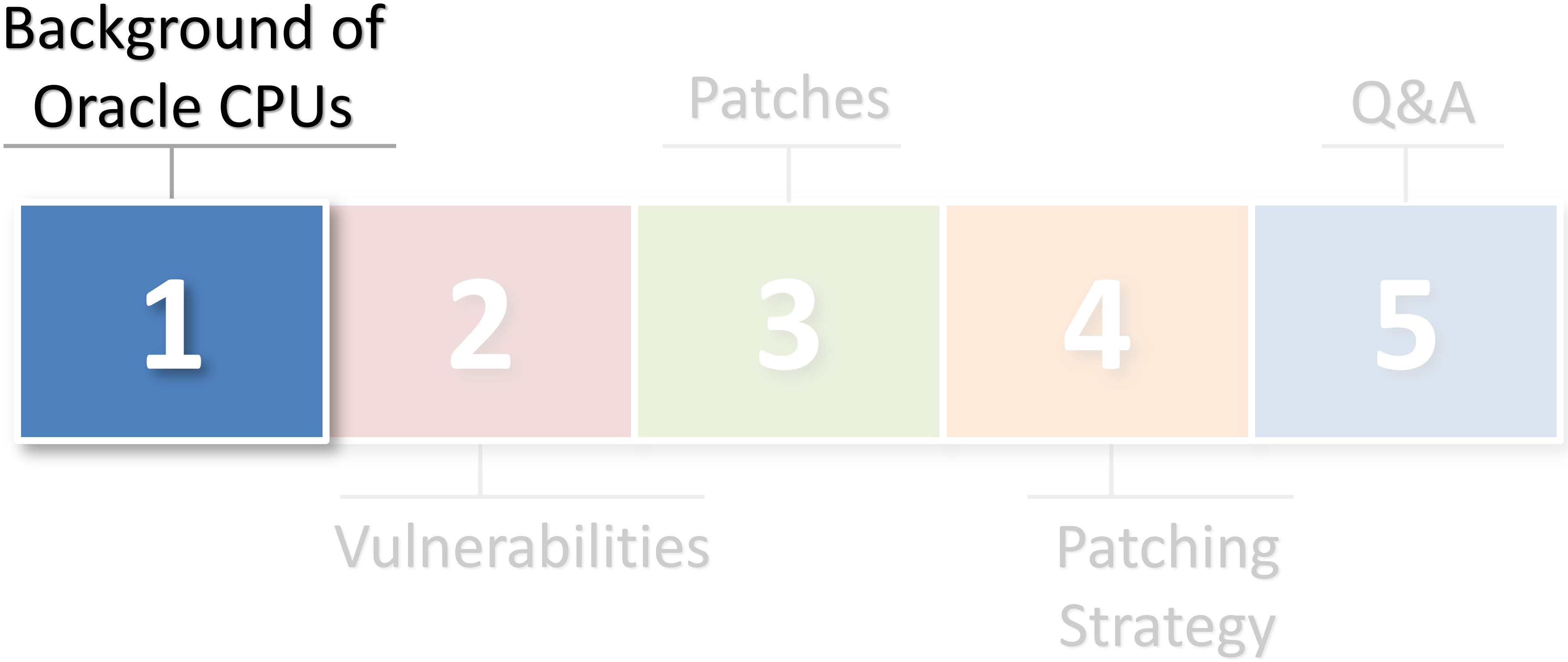
4

5

Vulnerabilities

Patching Strategy

Agenda



1 Background of Oracle CPUs

2 Vulnerabilities

3 Patches

4 Patching Strategy

5 Q&A

Oracle Critical Patch Updates

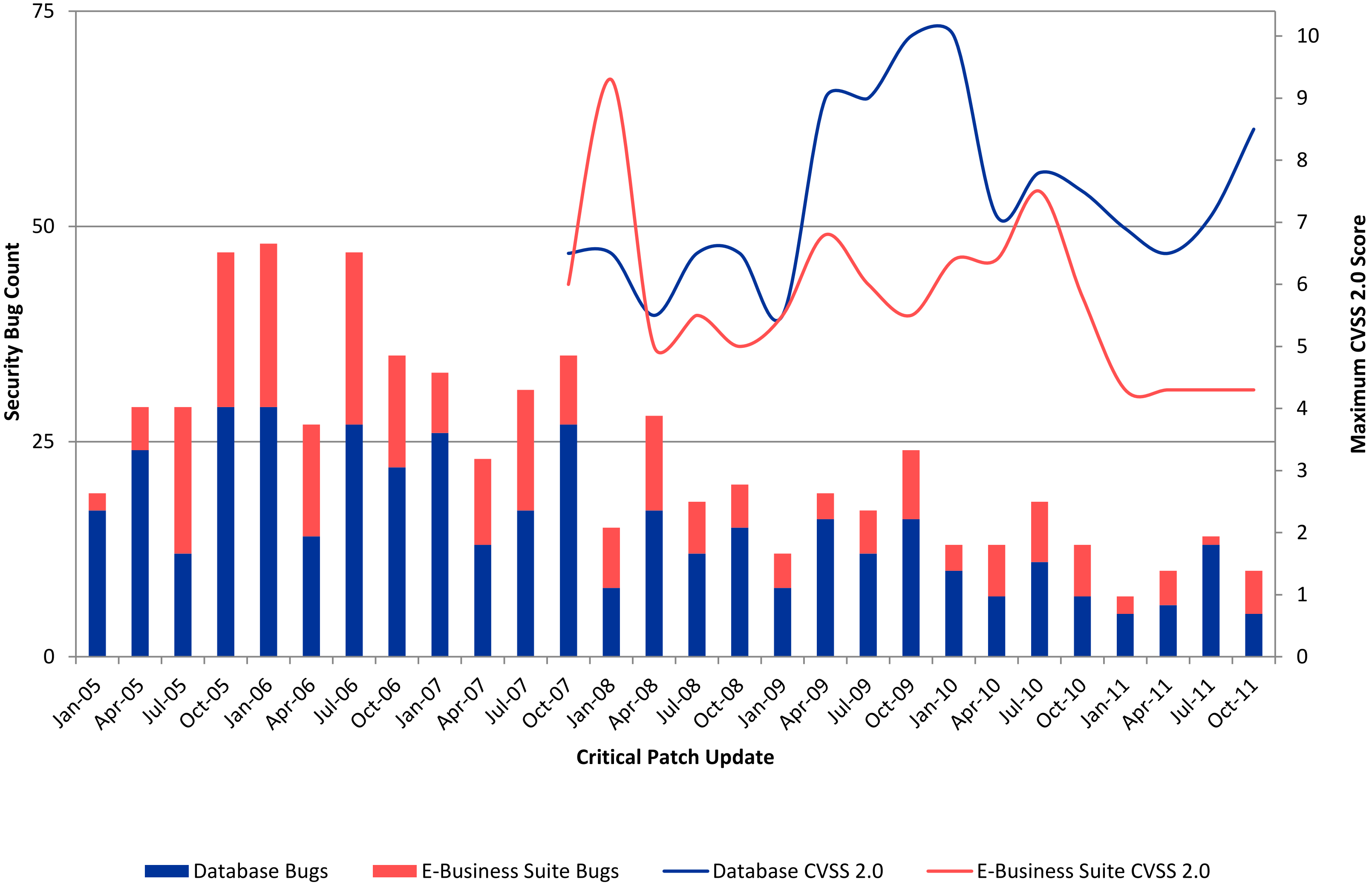
Fixes for security bugs in all Oracle products

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

Twenty-eight CPUs released to date starting with January 2005

- 1,334 security bugs fixed (average is 48 bugs per CPU)
- 425 bugs in the Oracle Database
- 229 bugs in the Oracle E-Business Suite

Oracle Security Bugs per Quarter



INTEGRIGY

Oracle Security Bug Process

Bug reported

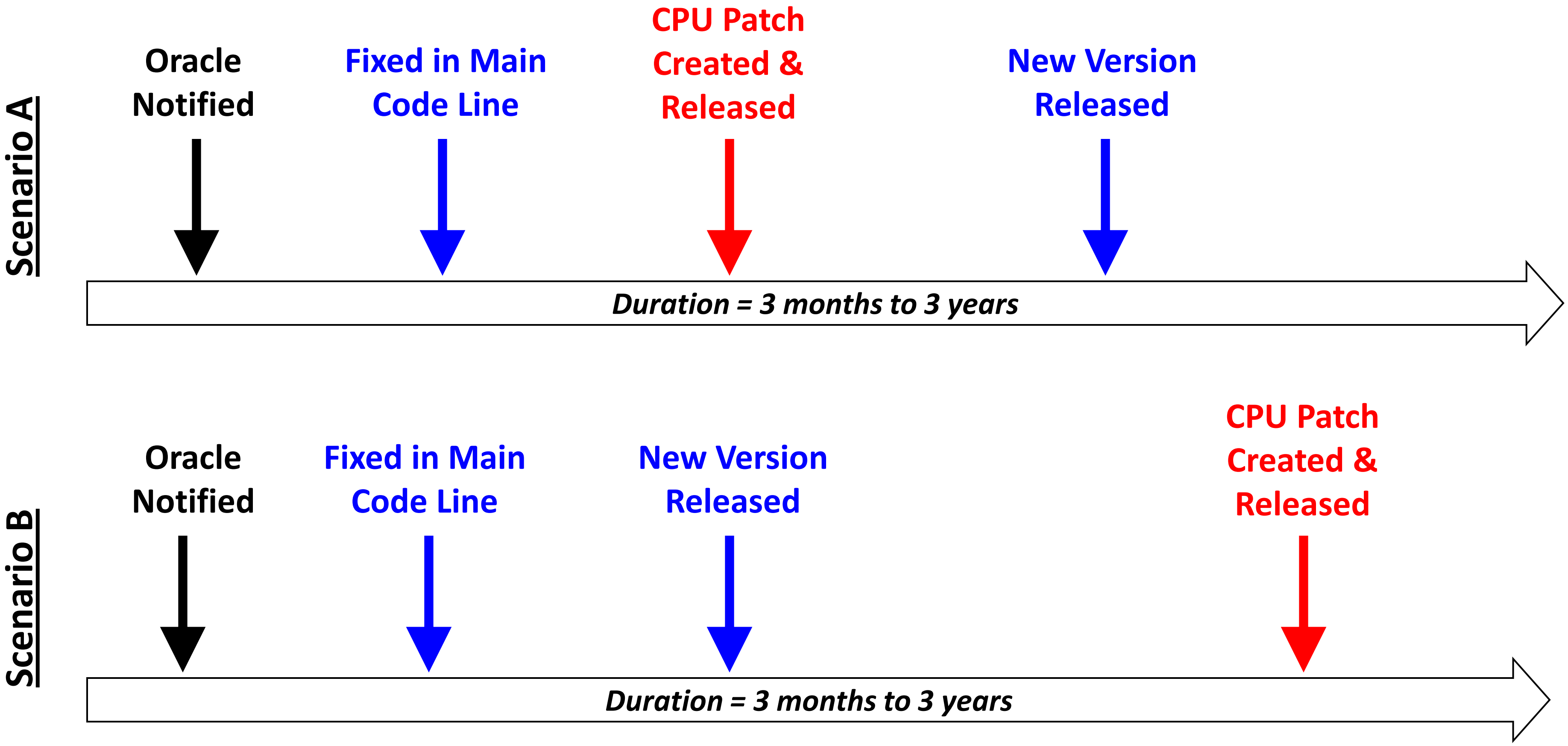
Elapsed time on average is 18 months

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

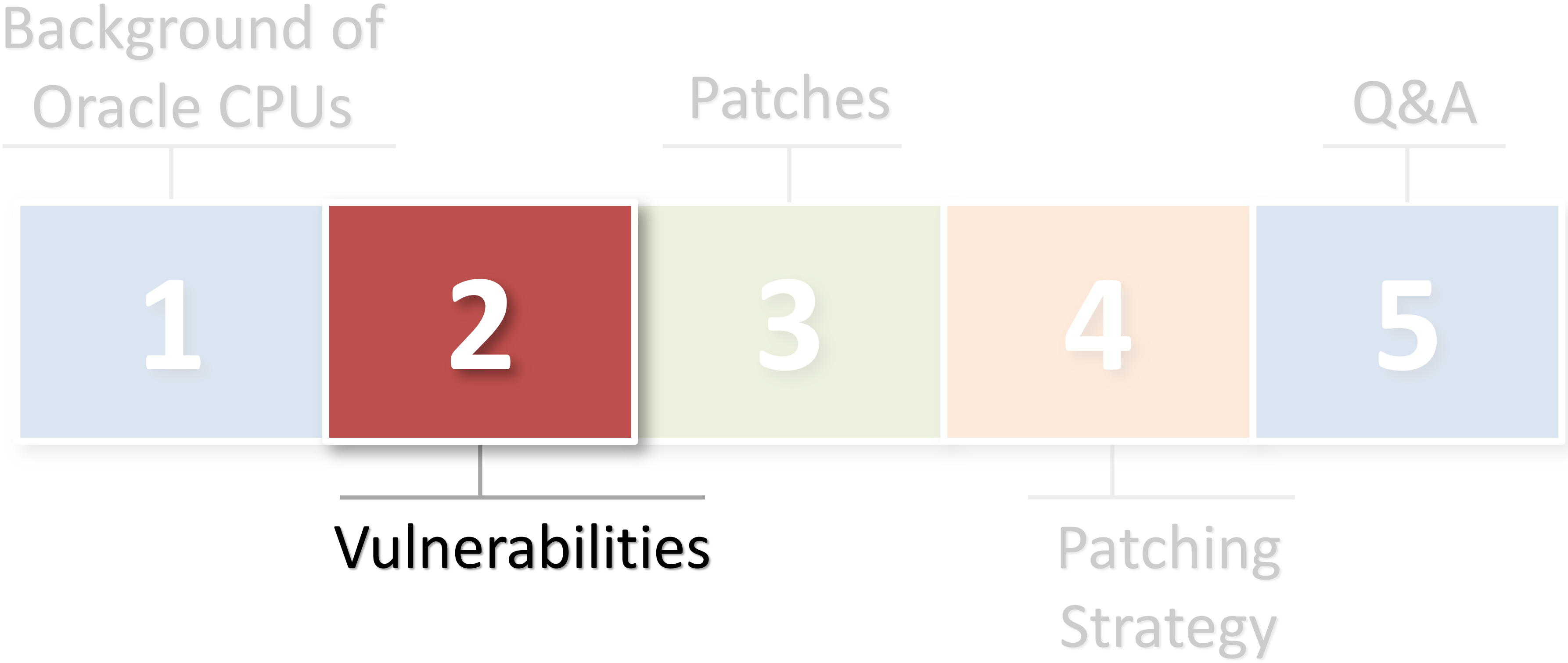
CPU Patch Created & Released

Duration = 3 months to 3 years

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



1 Background of Oracle CPUs

2 Vulnerabilities

3 Patches

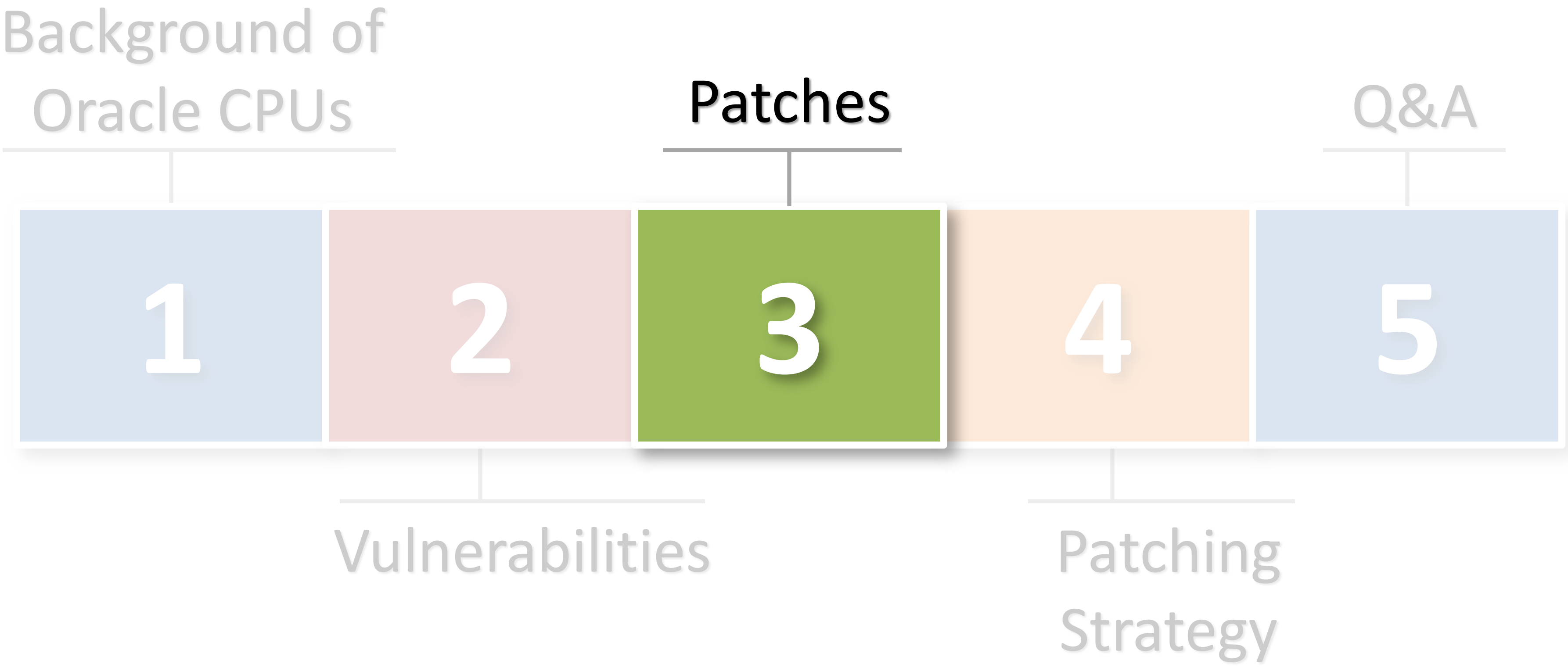
4 Patching Strategy

5 Q&A

Oracle Database Vulnerabilities (October 2011)

CVE	Component	Notes
CVE-2011-2301	**Oracle Text**	▪ **Buffer overflow in library** ▪ TABLEFUNC_ASOWN function in CTXSYS.DRVDISP ▪ Execute on CTXSYS.DRVDISP or EXECUTE ANY PROC ▪ Fully compromise Windows server – limited to oracle account on Unix/Linux
CVE-2011-3512	**Core RDBMS**	▪ **SQL Injection in handling of Spatial Indexes** ▪ Requires Create Procedure and Create Table ▪ Elevate to SYSDBA
CVE-2011-3511 CVE-2011-2322	**Database Vault**	▪ **Circumvent Database Vault Protections** ▪ Requires SYSDBA or DV_ACCTMGR role ▪ Change any password using OCIPasswordChange API

Agenda



1 Background of Oracle CPUs

2 Vulnerabilities

3 Patches

4 Patching Strategy

5 Q&A

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

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)(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	July 2012 (a)

(a) Oracle CPU Support Date (b) Oracle Lifetime Support Date
(c) Supported only on limited platforms

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**
- **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';
```

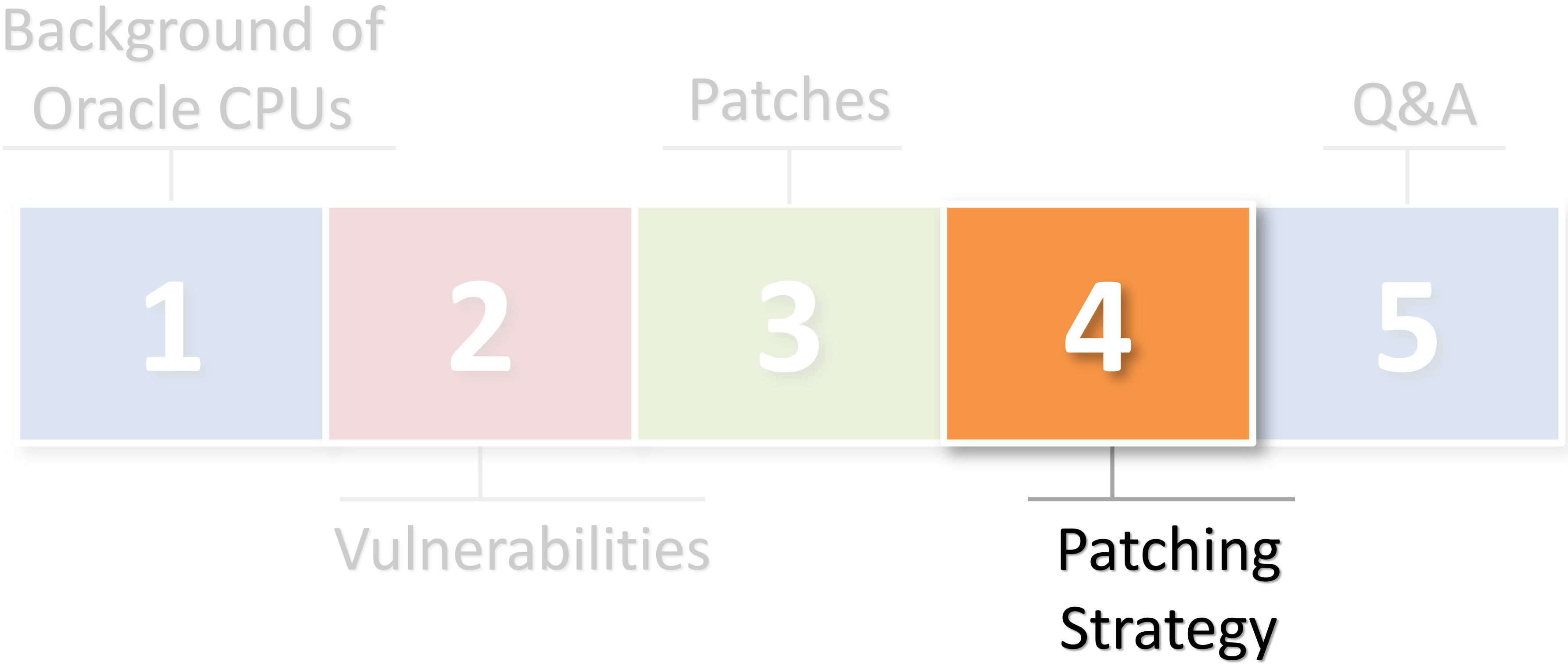
OPatch

- **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
```

Agenda



1 Background of Oracle CPUs

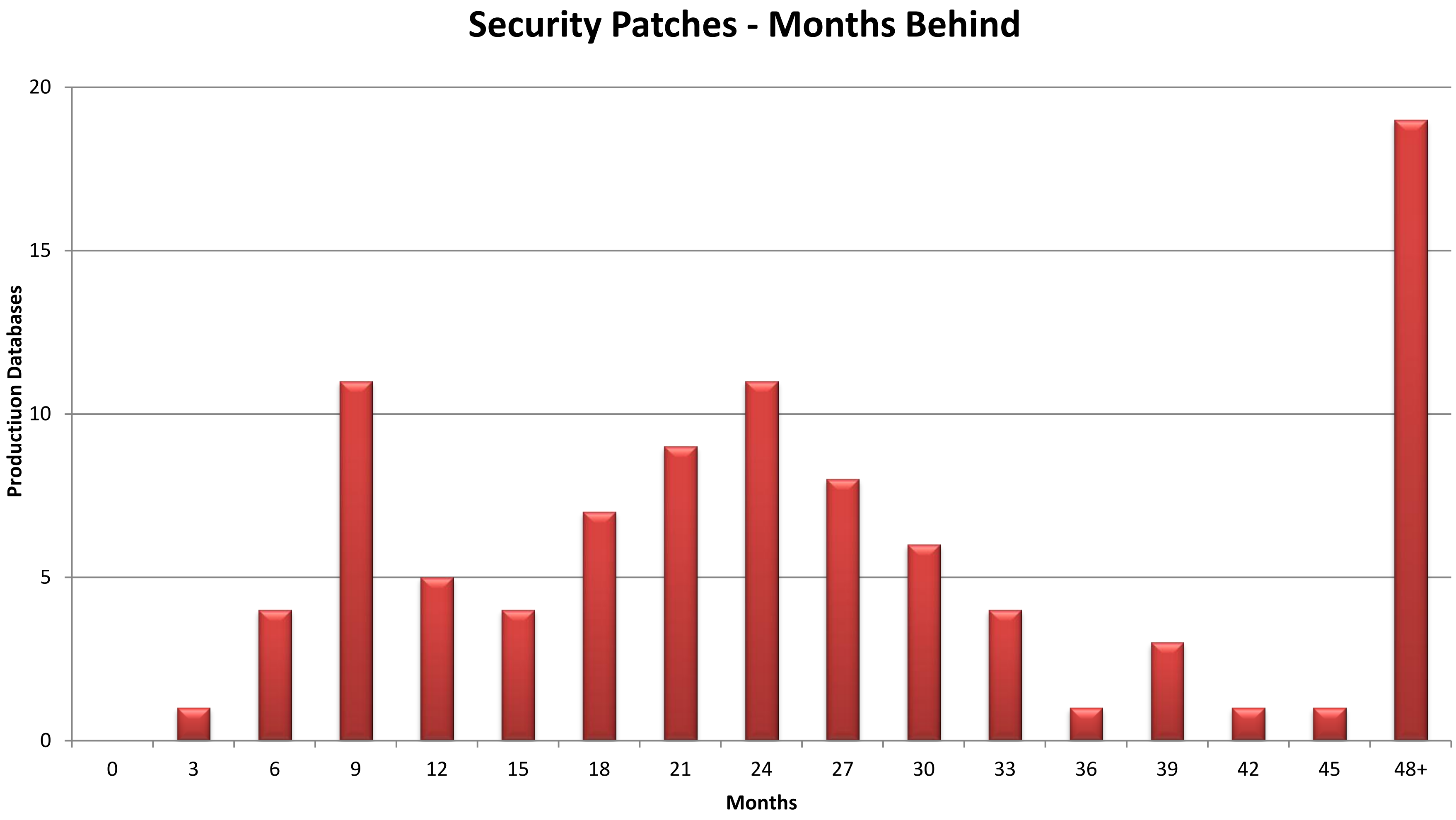
2 Vulnerabilities

3 Patches

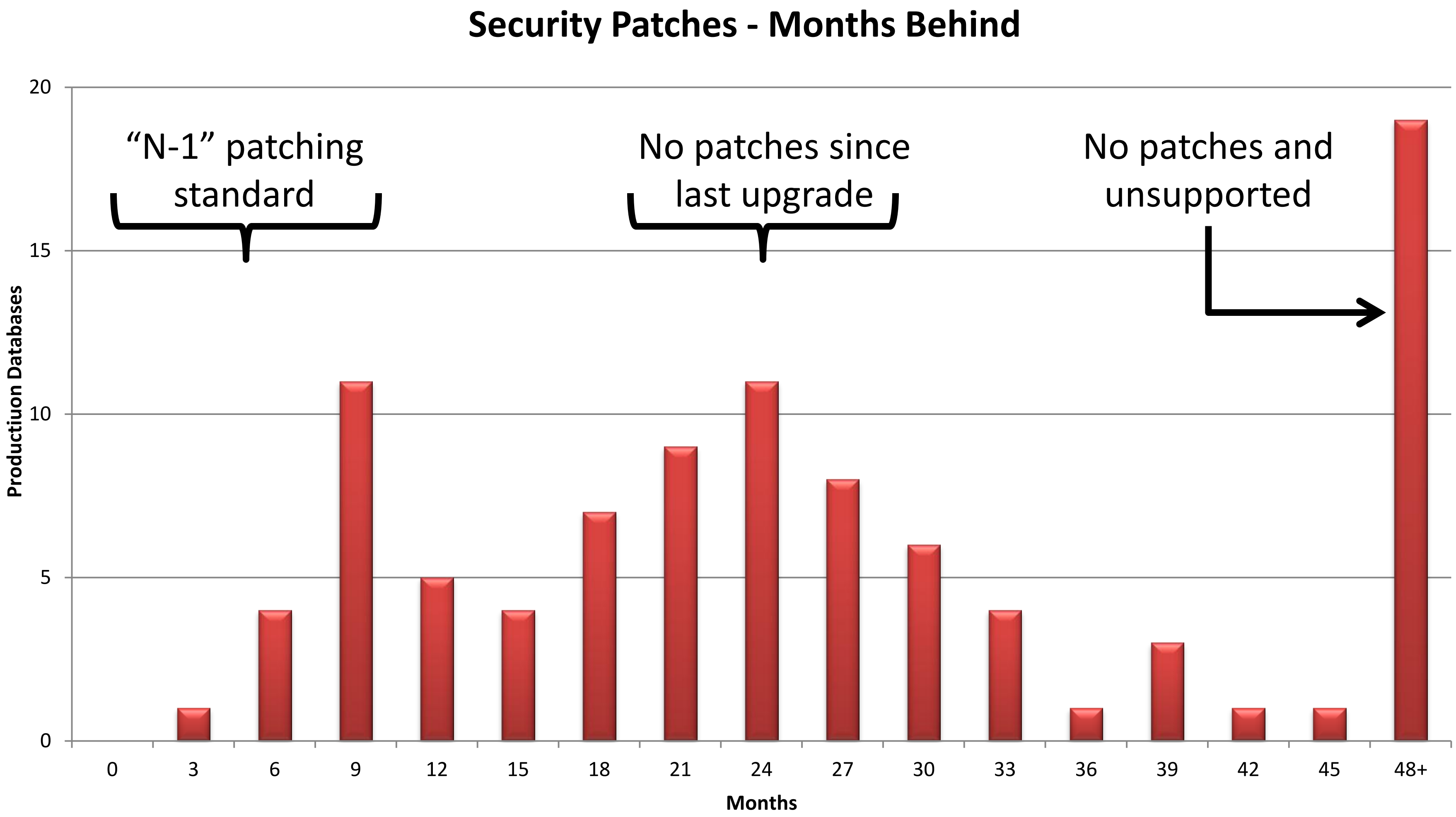
4 Patching Strategy

5 Q&A

Oracle CPU Patching Metric



Oracle CPU Patching Metric



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
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

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 complier 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 (July 2010)
  - Upgrade database to new version or patchset (9.2.0.8 to 10.2.0.4 or 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 July 2010 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
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

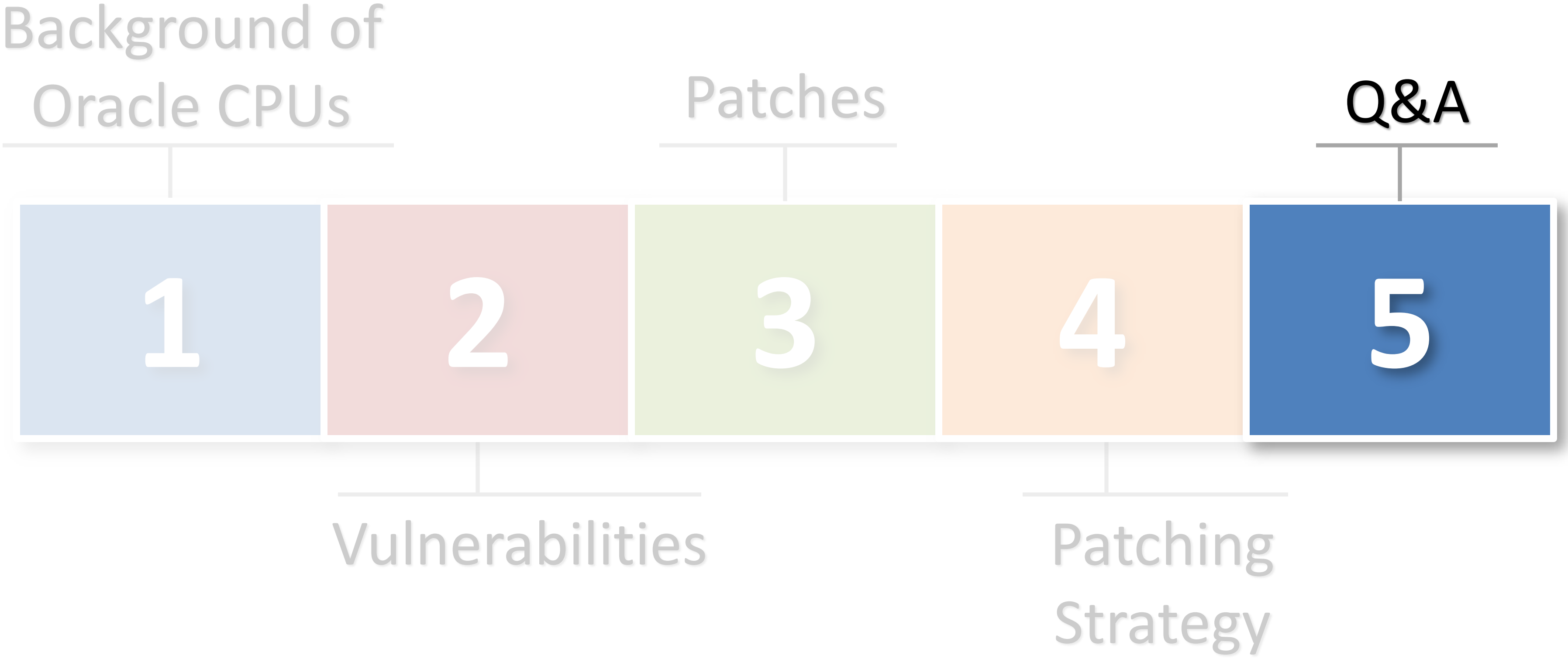
#3 ORACLE_HOME vs. Database

- **Scenario**
  - Latest CPU patch is applied (July 2010) to ORACLE_HOME
  - Install a new database from the patched ORACLE_HOME
- **Do I have to run the *catcpu.sql* from the July 2010 CPU?**
  - Yes, a few 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 (July 2010) 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 July 2010 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*

Agenda



Background of Oracle CPUs

Vulnerabilities

Patches

Patching Strategy

Q&A

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