# Oracle Critical Patch Update
# October 2011
# E-Business Suite Impact

**Stephen Kost**
**Chief Technology Officer**
**Integrigy Corporation**

**Phil Reimann**
**Director of Business Development**
**Integrigy Corporation**

**October 27, 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

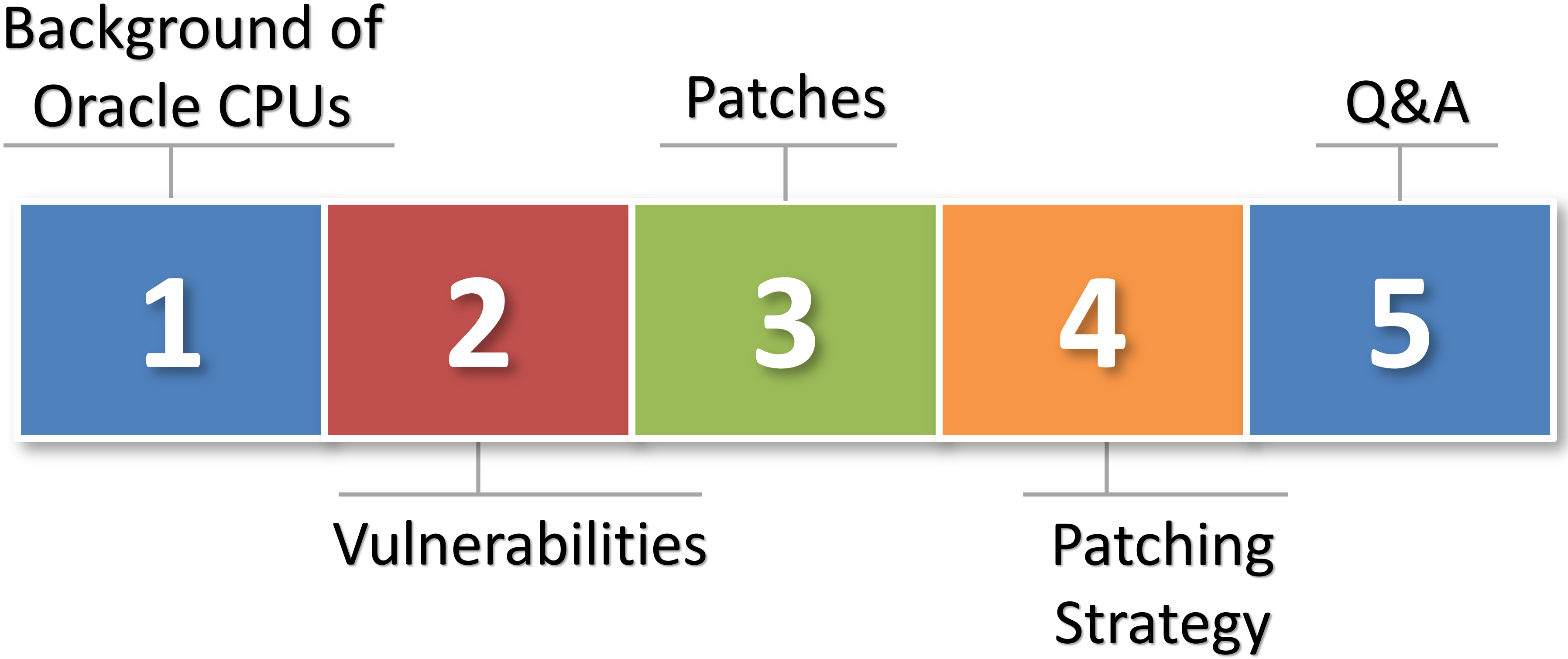
- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

INTEGRIGY

# Integrigy Security Alerts

| Security Alert | Versions | Security Vulnerabilities |
|---|---|---|
| **Critical Patch Update July 2008** | **Oracle 11g**<br>**11.5.8 – 12.0.x** | ▪ 2 Issues in Oracle RDBMS Authentication<br>▪ 2 Oracle E-Business Suite vulnerabilities |
| **Critical Patch Update April 2008** | **12.0.x**<br>**11.5.7 – 11.5.10** | ▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc. |
| **Critical Patch Update July 2007** | **12.0.x**<br>**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**<br>**11.0.x** | ▪ Default configuration issues |
| **Critical Patch Update July 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities<br>▪ Information disclosure |
| **Critical Patch Update April 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities<br>▪ Information disclosure |
| **Critical Patch Update Jan 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities |
| **Oracle Security Alert #68** | **Oracle 8i, 9i, 10g** | ▪ Buffer overflows<br>▪ Listener information leakage |
| **Oracle Security Alert #67** | **11.5.1 – 11.5.8**<br>**11.0.x** | ▪ 10 SQL injection vulnerabilities |
| **Oracle Security Alert #56** | **11.5.1 – 11.5.8**<br>**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<br>▪ Obtain sensitive information (valid session) |
| **Oracle Security Alert #53** | **10.7, 11.0.x**<br>**11.5.1 – 11.5.8** | ▪ No authentication in FNDFS program<br>▪ Retrieve any file from O/S |

# Agenda



1 Background of Oracle CPUs

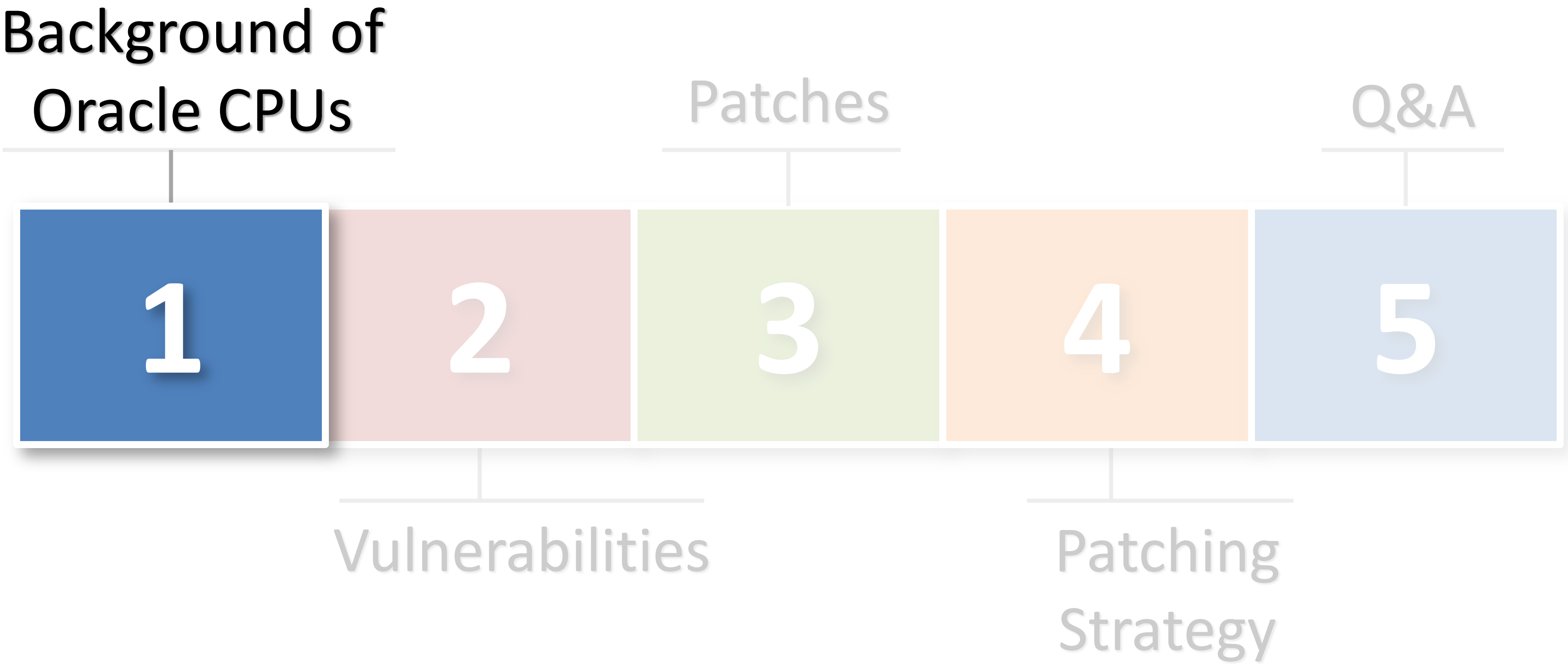
2 Vulnerabilities

3 Patches

4 Patching Strategy

5 Q&A

# Agenda



1 Background of Oracle CPUs

2 Vulnerabilities

3 Patches

4 Patching Strategy

5 Q&A

# Oracle Critical Patch Updates

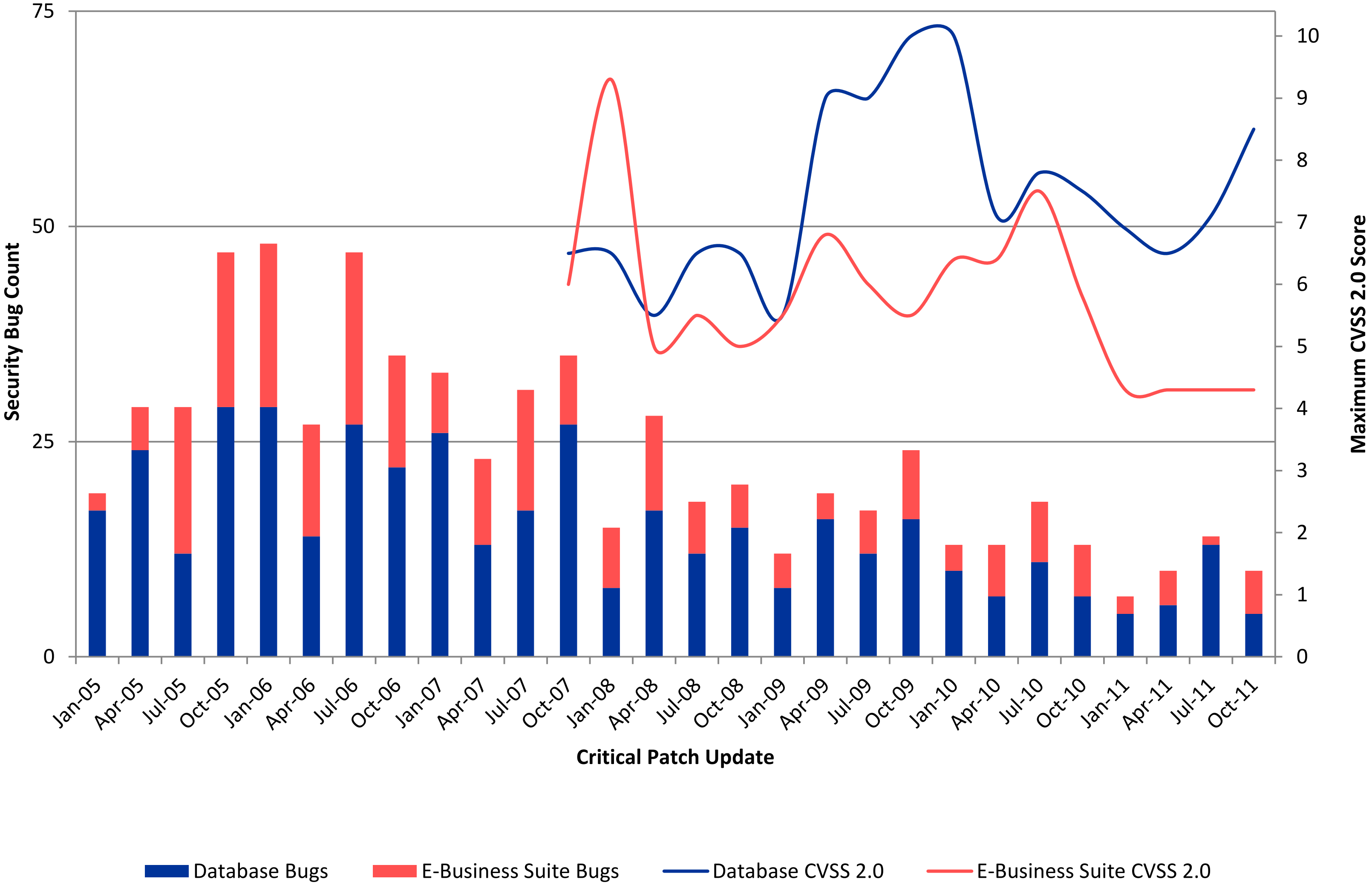
**Fixes for security bugs in all Oracle products**

- 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

# 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

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

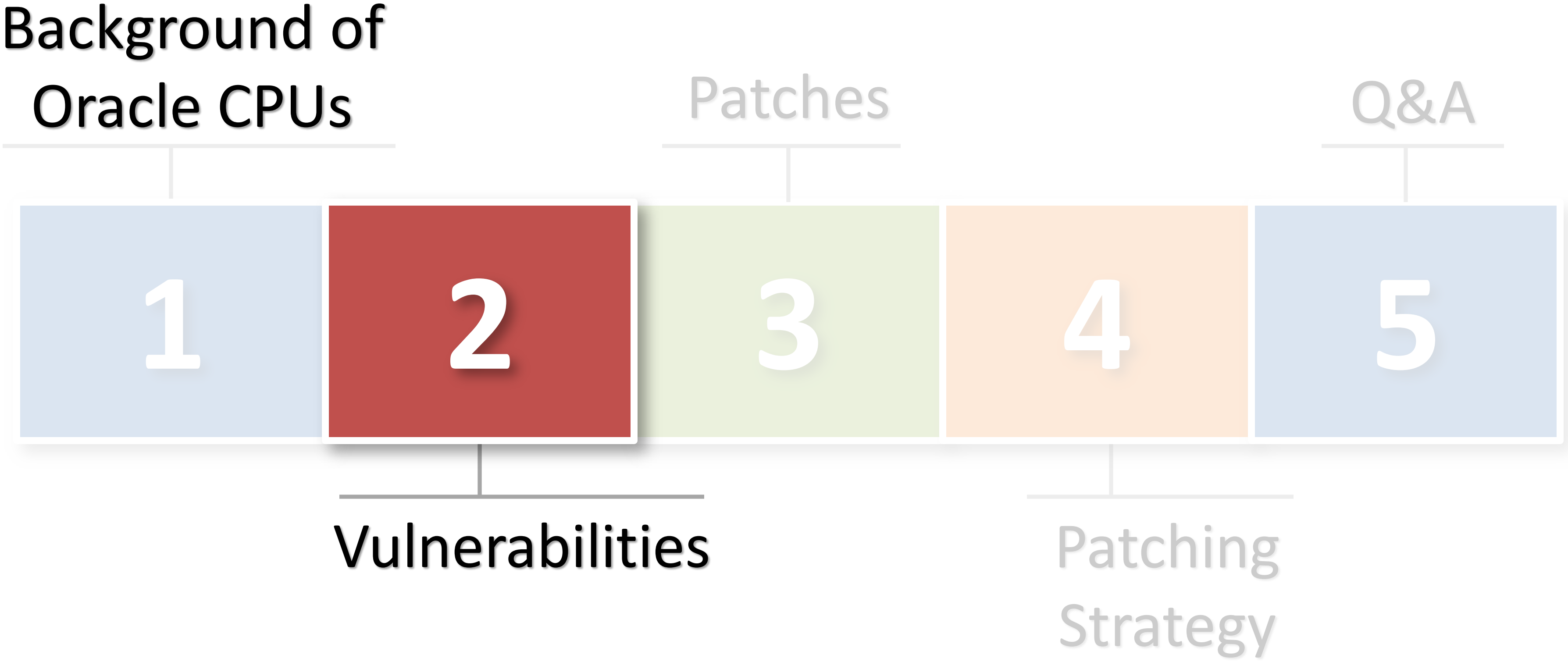
4. **Oracle includes fix in quarterly CPU**
   - **From initial report to security patch release is 3 months to 3 years**

INTEGRIGY

# 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

Vulnerabilities

Patches

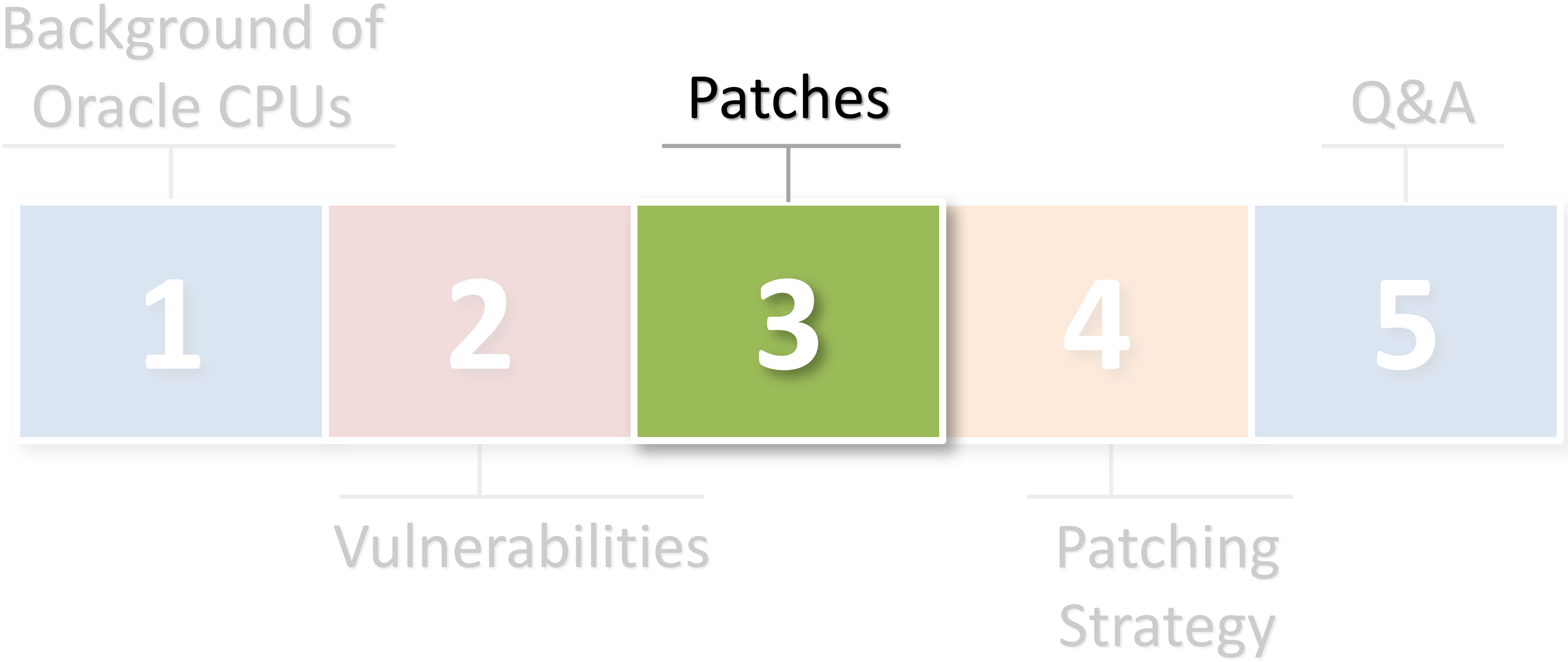
Patching Strategy

Q&A

# Oracle Database Vulnerabilities (October 2011)

| CVE | Component | Notes |
|---|---|---|
| CVE-2011-2301 | **Oracle Text** | ▪ **Buffer overflow in library?**<br>▪ Execute on CTXSYS.DRVDISP<br>▪ Fully compromise Windows server – limited to oracle account on Unix/Linux |
| CVE-2011-3512 | **Core RDBMS** | ▪ **Buffer overflow in library?**<br>▪ Requires Create session, create procedure, create table |
| CVE-2011-3511<br>CVE-2011-2322 | **Database Vault** | ▪ **Circumvent Database Vault**<br>▪ Requires a privileged user or SYSDBA |

# 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**

INTEGRIGY

# 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

# 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 (October 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 (Oct 2011) | | October 2011 | October 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
  - October 2011 requires RUP6 or RUP7
- **Oracle E-Business Suite 12.0**
  - October 2011 requires 12.0.4 + ATG 12.0.6
- **Oracle E-Business Suite 12.1**
  - October 2011 requires 12.1.1 + ATG 12.1.2

# 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 (October 2011)

| CVE | Importance | Fix Complexity | Notes |
|---|---|---|---|
| CVE-2011-3513 | Medium | Medium | **Application Object Library - HTML Pages**<br>▪ Security vulnerabilities in common Marlin<br>▪ Remotely exploitable without authentication<br>▪ Minimal testing of basic OA Framework pages<br>▪ Recommended for all implementations<br>▪ **This page is not blocked by the URL firewall for external access** |
| CVE-2011-2308 | Medium | Low | **Application Object Library – Online Help**<br>▪ 12.0.x and 12.1.x only<br>▪ Security vulnerabilities in Online Help<br>▪ Remotely exploitable without authentication<br>▪ No testing required for on-line help<br>▪ Recommended for all implementations<br>▪ **This page is not blocked by the URL firewall for external access** |

# Oracle E-Business Suite Vulnerabilities (October 2011)

| CVE | Importance | Fix Complexity | Notes |
|---|---|---|---|
| CVE-2011-2302 | Medium | Medium | **Application Object Library – Single Signon**<br>▪ Security vulnerabilities in Single Signon<br>▪ Remotely exploitable without authentication<br>▪ Flow testing of all Single Signon<br>▪ Recommended for all Single Signon implementations<br>▪ **This page is not blocked by the URL firewall for external access** |
| CVE-2011-2303 | Medium | Low | **Application Object Library – Attachments and File Upload**<br>▪ Security vulnerabilities when attaching file<br>▪ Not remotely exploitable without authentication<br>▪ Basic testing of all file attachments and file upload<br>▪ Recommended for all implementations<br>▪ **This page is not blocked by the URL firewall for external access** |

# Oracle E-Business Suite Vulnerabilities (October 2011)

| CVE | Importance | Fix Complexity | Notes |
|---|---|---|---|
| CVE-2011-3519 | Low | Low | **Application Object Library – REST Services**<br>▪ 12.1.2 and 12.1.3 only<br>▪ Security vulnerability in REST Service<br>▪ Not remotely exploitable without authentication<br>▪ Testing of REST Services only if used<br>▪ Suggested for all implementations<br>▪ **This page is blocked by the URL firewall for external access** |

# Oracle E-Business Suite Vulnerabilities (October 2011)

| | | | |
|---|---|---|---|
| **CVE** | **CVE-2011-3513** | **Module** | **Application Object Library HTML Pages** |
| **Importance** | ◆ Medium | **Fix Complexity** | ◆ Low |
| **Remotely Exploitable** | ◆ Yes | **Blocked by URL Firewall** | ◆ Yes |

## Description

- Recommended for all implementations.

## Testing Required

- Basic testing of OA Framework pages as the underlying Marlin

# Oracle E-Business Suite Vulnerabilities (October 2011)

| | | | |
|---|---|---|---|
| **CVE** | **CVE-2011-2308** | **Module** | **Application Object Library Online Help** |
| **Importance** | ◆ Medium | **Fix Complexity** | ◆ Low |
| **Remotely Exploitable** | ◆ Yes | **Blocked by URL Firewall** | ◆ Yes |

## Description

- 12.0.x and 12.1.x only.
- Recommended for all implementations.

## Testing Required

- Only limited testing of the online help.

INTEGRIGY

# Oracle E-Business Suite Vulnerabilities (October 2011)

| | | | |
|---|---|---|---|
| **CVE** | **CVE-2011-2302** | **Module** | **Application Object Library Single Signon** |
| **Importance** | ◆ High | **Fix Complexity** | ◆ High |
| **Remotely Exploitable** | ◆ Yes | **Blocked by URL Firewall** | ◆ No |

| **Description** |
|---|
| |

| **Testing Required** |
|---|
| |

# Oracle E-Business Suite Vulnerabilities (October 2011)

| | | | |
|---|---|---|---|
| **CVE** | **CVE-2011-2303** | **Module** | **Application Object Library<br>File Upload/Attachments** |
| **Importance** | 🟨 Medium | **Fix Complexity** | 🟩 Low |
| **Remotely Exploitable** | 🟨 No | **Blocked by URL Firewall** | 🟥 No – OA Framework |

## Description

- Security vulnerability in the common file upload and attachment capabilities.
- Recommended for all implementations.

## Testing Required

- Testing of all file upload and attachments as the common Java classes and PL/SQL packages for file upload/attachments are updated.

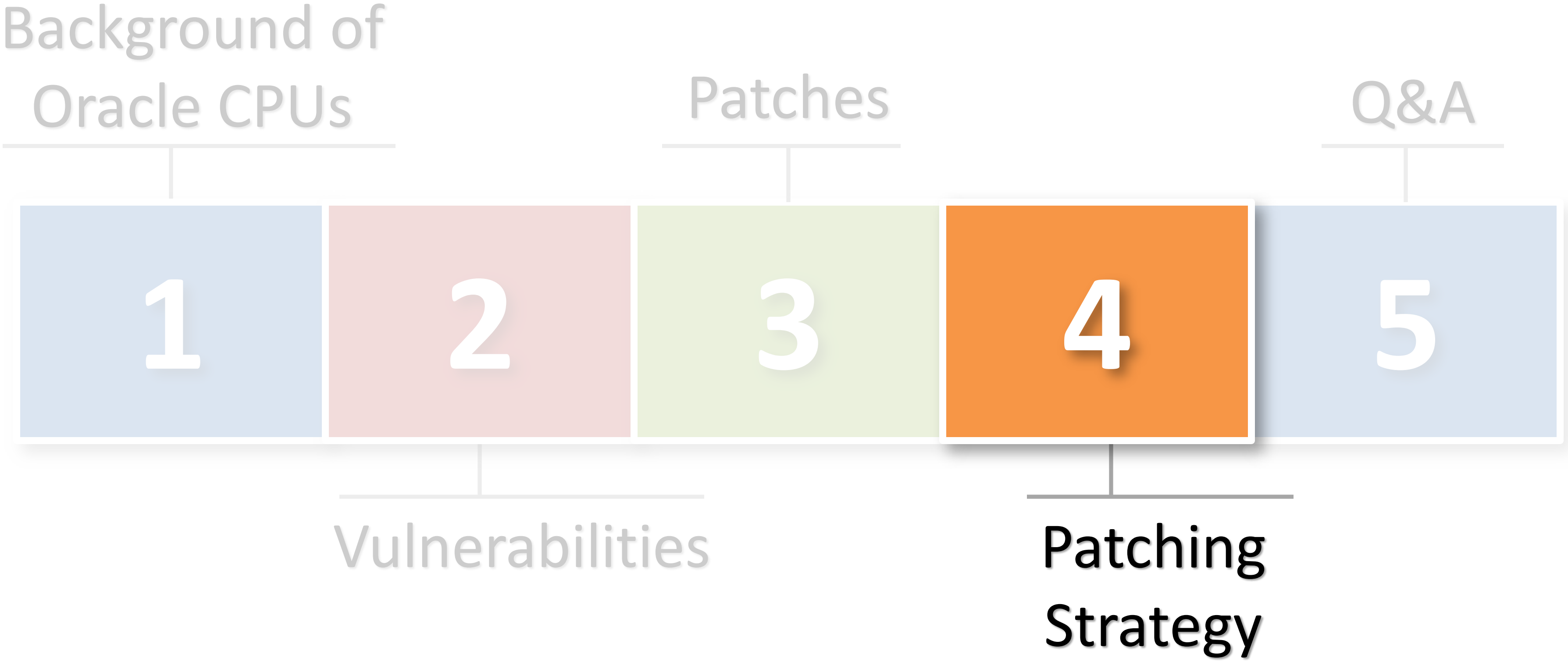
# Oracle E-Business Suite Vulnerabilities (October 2011)

| | | | |
|---|---|---|---|
| **CVE** | **CVE-2011-3519** | **Module** | **Application Object Library REST Services** |
| **Importance** | ◆ Medium | **Fix Complexity** | ◆ Low |
| **Remotely Exploitable** | ◆ No | **Blocked by URL Firewall** | ◆ No – OA Framework |

| **Description** |
|---|
| ▪ 12.1.x only |

| **Testing Required** |
|---|
| ▪ REST Services and authentication of services if used. |

# Agenda



1 Background of Oracle CPUs

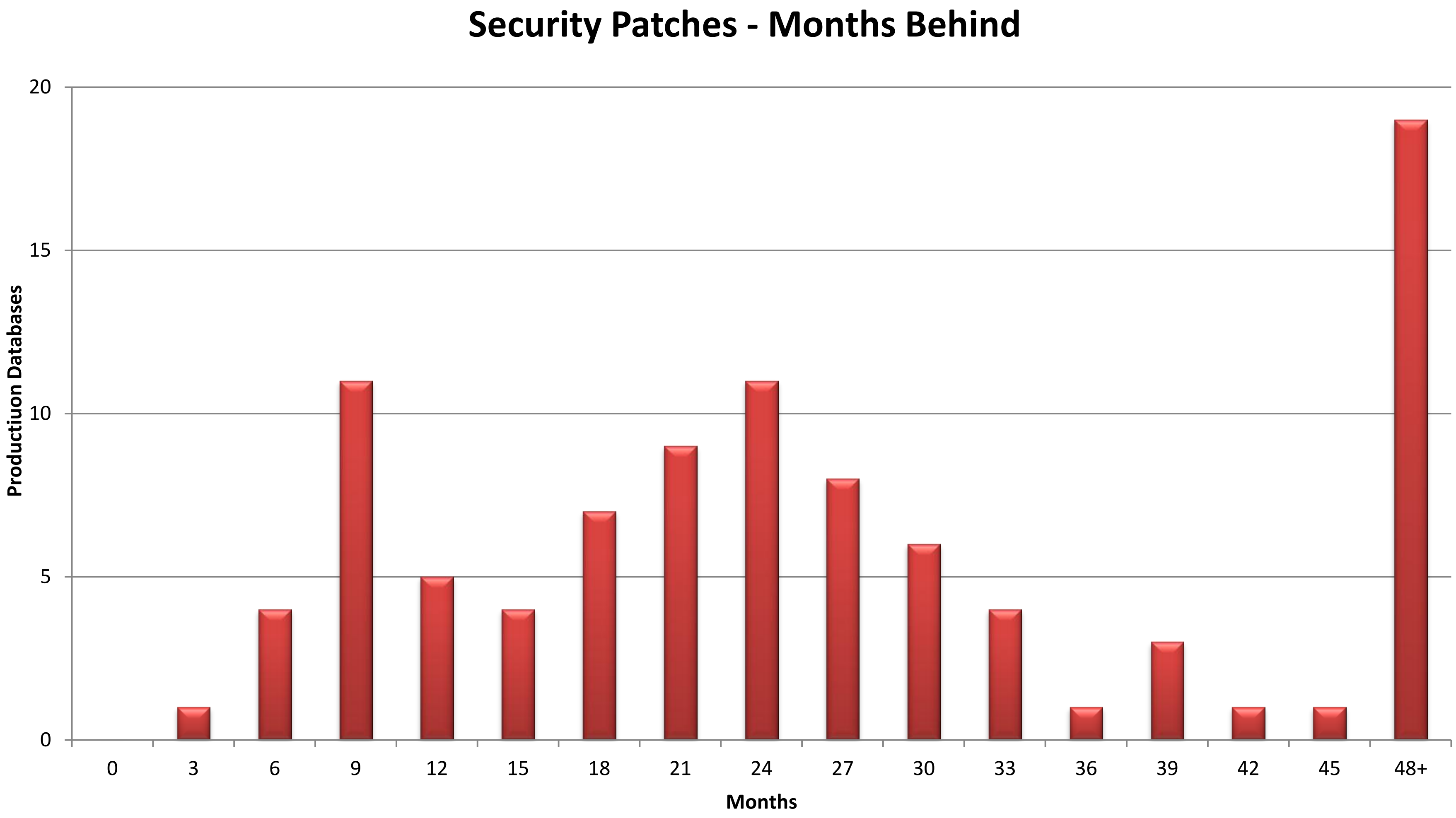
2 Vulnerabilities

3 Patches

4 Patching Strategy

5 Q&A

# Oracle CPU Patching Metric

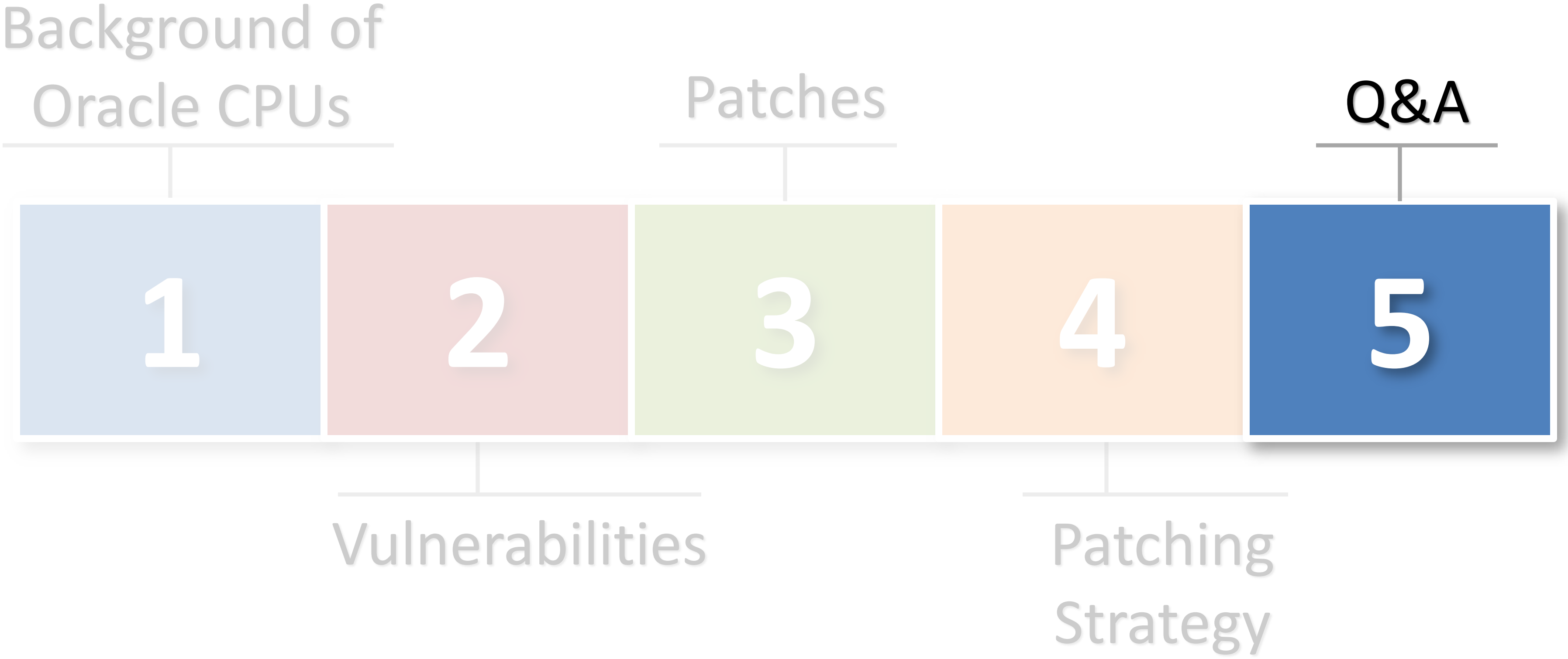


INTEGRIGY

# 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



1 Background of Oracle CPUs

2 Vulnerabilities

3 Patches

4 Patching Strategy

5 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