Oracle Security Vulnerabilities Dissected

An inside look at Oracle Critical Patch Updates and the security bugs fixed by the SPU and PSU patches

Stephen Kost
Chief Technology Officer
Integrigy Corporation

REMINDER

Check in on the
COLLABORATE mobile app

Agenda

Critical Patch Update Overview

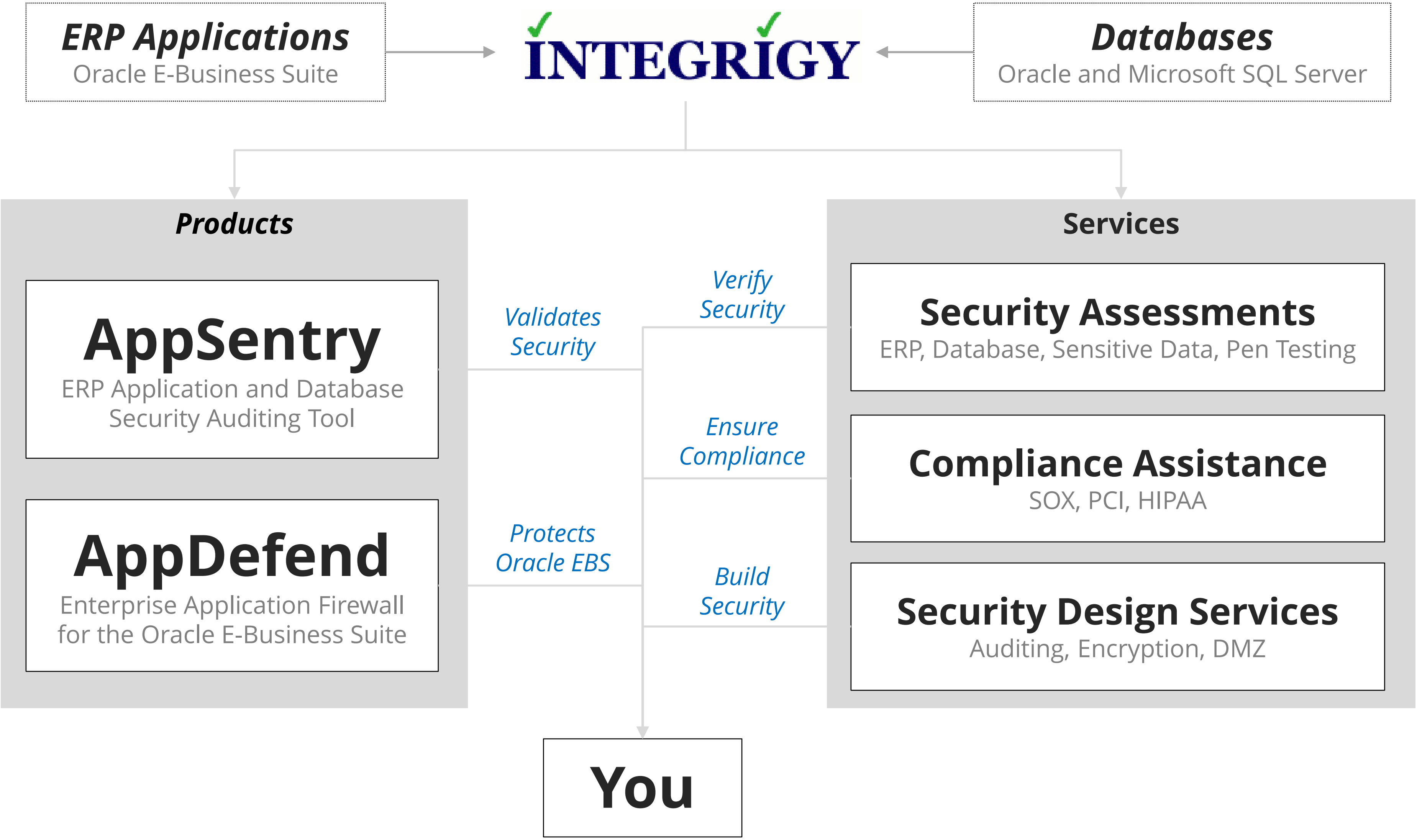
Reading the CPU Advisory

CVE-2012-1675
TNS Poisoning

Stealth Password Cracking
CVE-2012-3137

Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle and Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance
SOX, PCI, HIPAA

Build Security

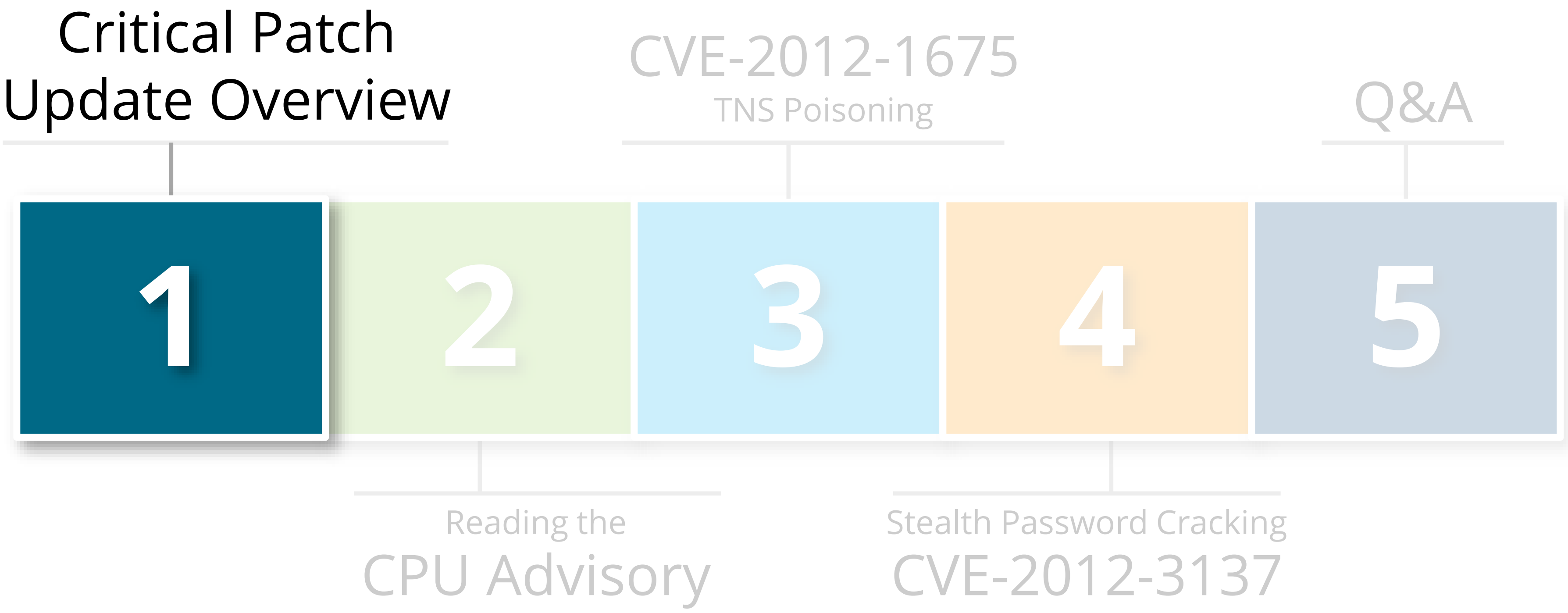
Security Design Services
Auditing, Encryption, DMZ

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

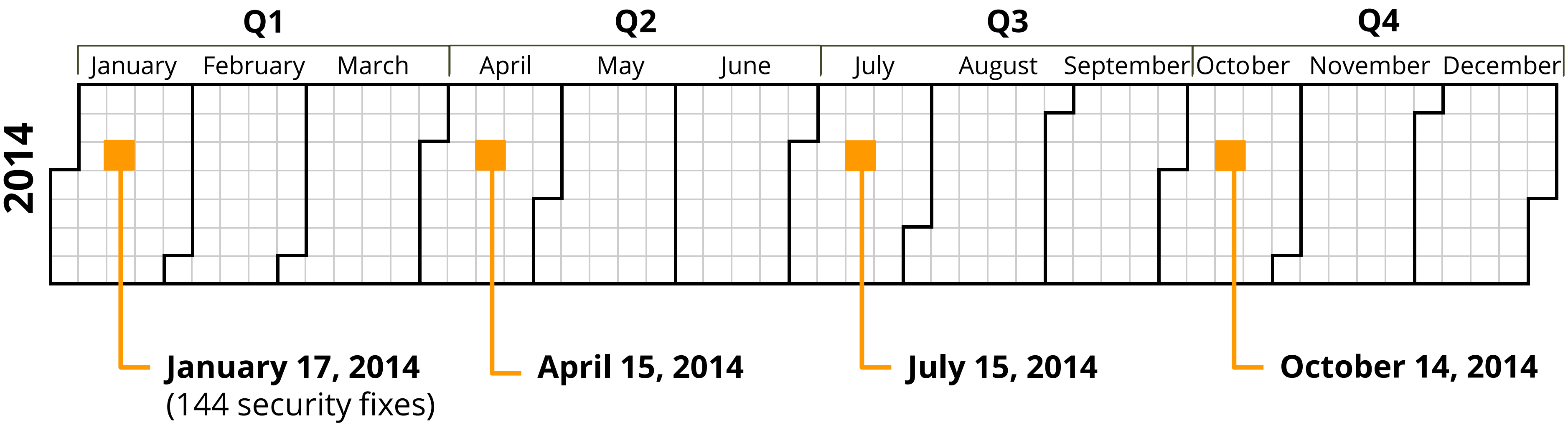
Agenda



1. Critical Patch Update Overview
2. Reading the CPU Advisory
3. CVE-2012-1675 TNS Poisoning
4. Stealth Password Cracking CVE-2012-3137
5. Q&A

Oracle Critical Patch Updates

- **Fixes for security bugs in all Oracle products**
  - Across all products including Solaris and Java
- **Released quarterly on a fixed schedule**
  - Tuesday closest to the **17th** day of January, April, July, and October



January 17, 2014
(144 security fixes)

April 15, 2014

July 15, 2014

October 14, 2014

37 Oracle Critical Patch Updates released since **January 2005**

Total security vulnerabilities **1,795** average of 49 per CPU

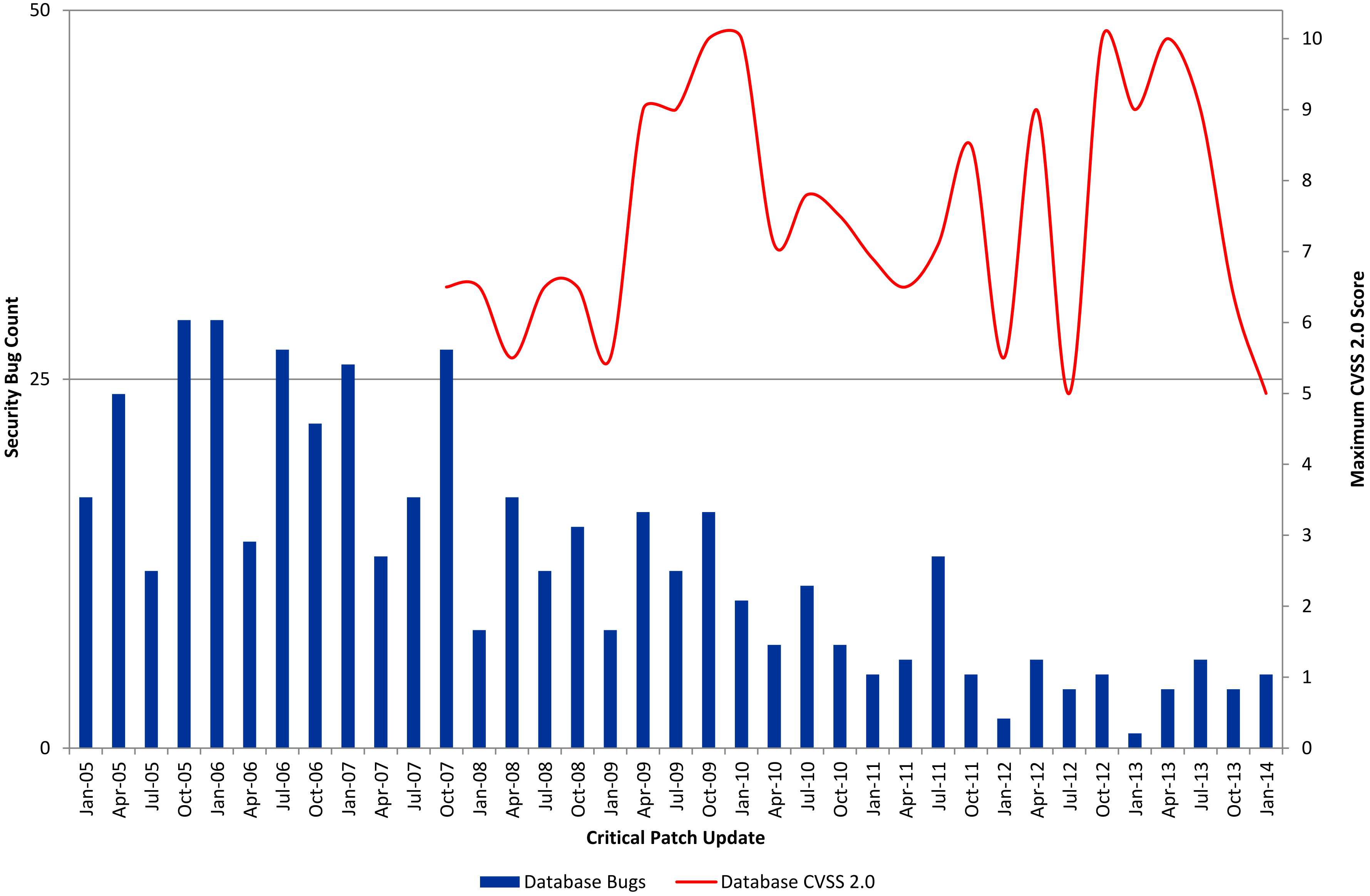
464

Oracle Database vulnerabilities

276

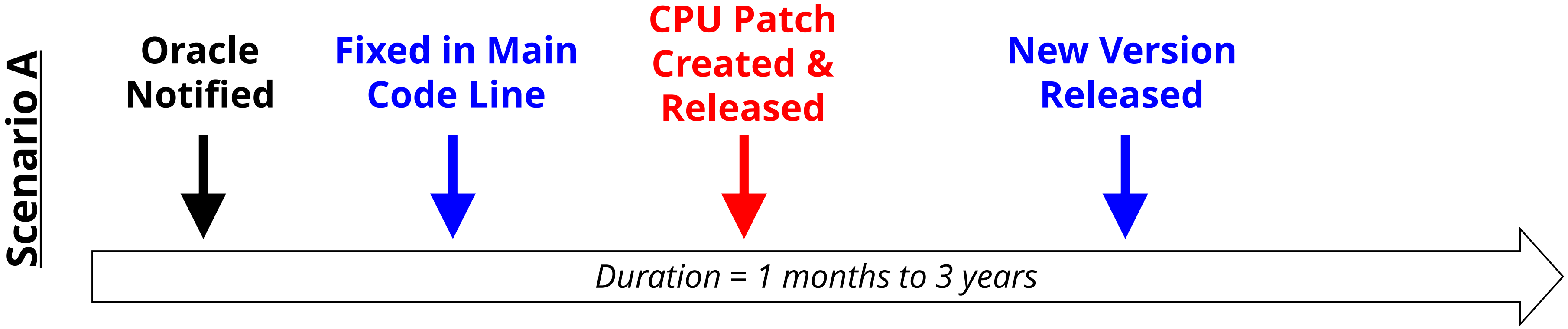
Oracle E-Business Suite vulnerabilities

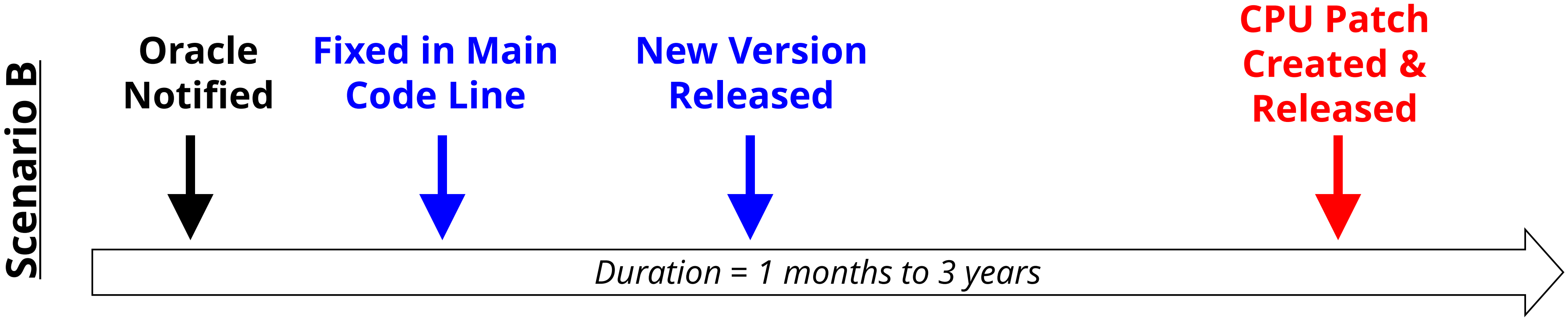
Oracle Security Bugs per Quarter



Oracle Security Bug Process

Vulnerability may be fixed first in a new version (e.g., 11.2.0.4) before through a Critical Patch Update with no notification





Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-11	**UPGRADE**	11.1.0.7	Upgraded from 11.1.0.6
18-JAN-12	APPLY	11.1.0.7	**CPUOct2011**
09-APR-13	**UPGRADE**	11.2.0.2	Upgraded from 11.1.0.7
18-AUG-13	APPLY	11.2.0.2	**CPUJul2013**
30-JAN-14	APPLY	11.2.0.2	**CPUJan2014**
06-APR-14	**UPGRADE**	11.2.0.3	Upgraded from 11.2.0.2

What CPU Level is this database patched to?

A. July 2011

B. October 2011

C. July 2013

D. January 2014

Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-11	**UPGRADE**	11.1.0.7	Upgraded from 11.1.0.6
18-JAN-12	APPLY	11.1.0.7	~~CPUOct2011~~
09-APR-13	**UPGRADE**	11.2.0.2	Upgraded from 11.1.0.7
18-AUG-13	APPLY	11.2.0.2	~~CPUJul2013~~
30-JAN-14	APPLY	11.2.0.2	~~CPUJan2014~~
27-FEB-14	**UPGRADE**	11.2.0.3	Upgraded from 11.2.0.2

What CPU Level is this database patched to?

[✓ A. July 2011] **B. October 2011**

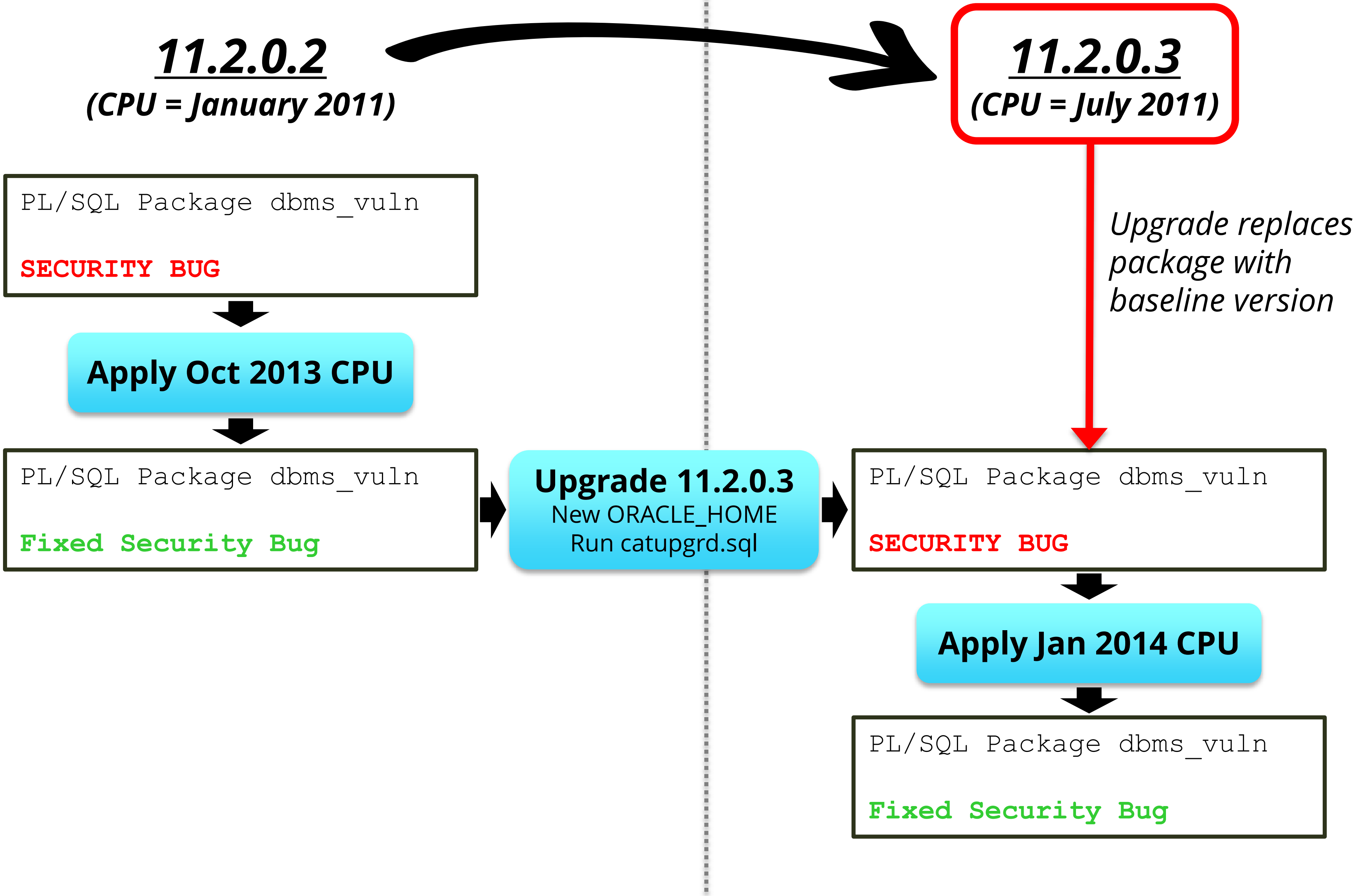
C. July 2013 **D. January 2014**

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
11.2.0.4	October 2013
12.1.0.1	July 2013

At time of release, usually the LATEST AVAILABLE CPU is included

CPU Baseline Illustrated



11.2.0.2

(CPU = January 2011)

11.2.0.3

(CPU = July 2011)

Upgrade replaces package with baseline version

PL/SQL Package dbms_vuln

SECURITY BUG

Apply Oct 2013 CPU

PL/SQL Package dbms_vuln

Fixed Security Bug

Upgrade 11.2.0.3

New ORACLE_HOME

Run catupgrd.sql

PL/SQL Package dbms_vuln

SECURITY BUG

Apply Jan 2014 CPU

PL/SQL Package dbms_vuln

Fixed Security Bug

Database CPU Support Dates

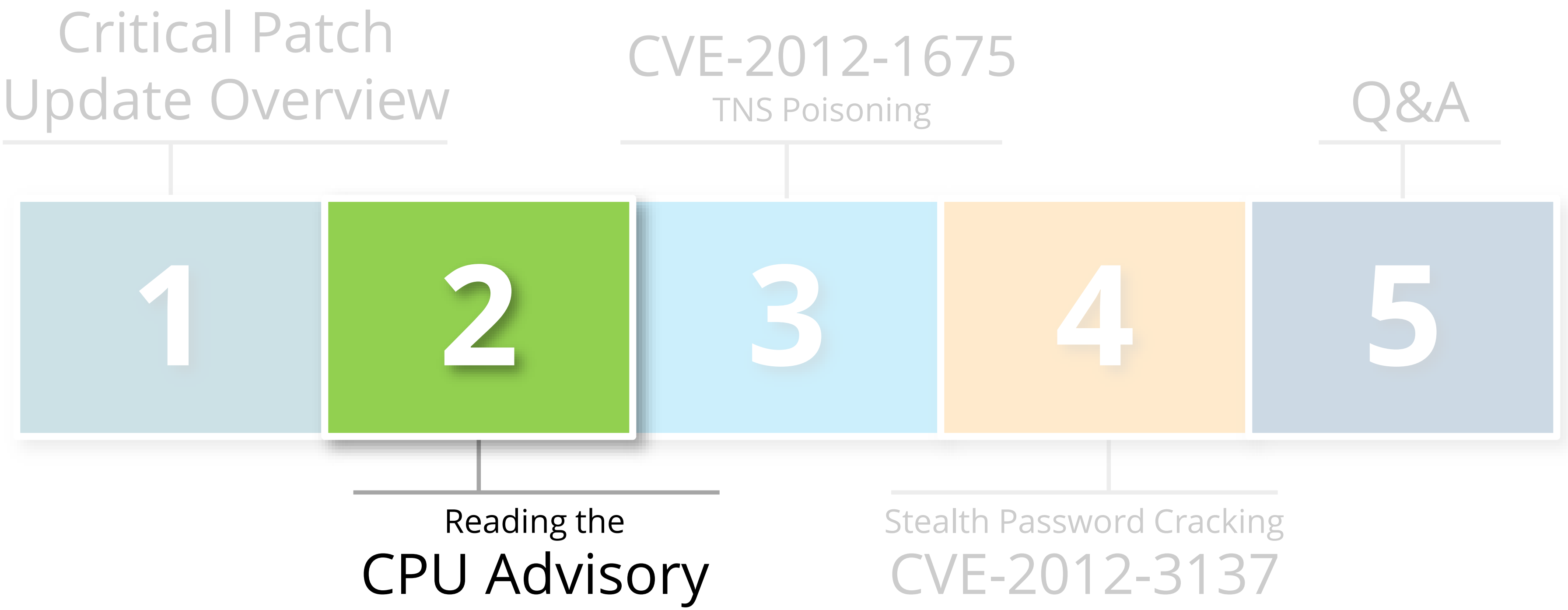
Database Version	*Terminal CPU*
10.1.0.5	**January 2012 (b)**
10.2.0.4	**July 2011 (a)(c)**
10.2.0.5	**July 2013 (b)**
11.1.0.7	**July 2015 (b)**
11.2.0.1	**July 2011 (a)**
11.2.0.2	**January 2013 (a)**
11.2.0.3	**July 2015 (a)**
11.2.0.4	**January 2018 (b)**

(a) Oracle CPU Support Date

(b) Oracle Lifetime Support Date

(c) Supported only on limited platforms

Agenda



1

Critical Patch
Update Overview

2

Reading the
CPU Advisory

3

CVE-2012-1675
TNS Poisoning

4

Stealth Password Cracking
CVE-2012-3137

5

Q&A

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-3137	**Oracle RDBMS**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
10.0	**Network**	**Low**	**None**	**Complete**	**Complete**	**Complete**	**10.2.0.3** **10.2.0.4** **10.2.0.5** **...**

CVE = Common Vulnerability Enumeration

Standard identifier assigned for security vulnerabilities. Each Oracle security vulnerability will have a unique CVE number.

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2014-0378	**Spatial**	**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	
4.1	**Local**	**Medium**	**Single**	**Partial**	**Partial**	**Partial**	**11.1.0.7** **11.2.0.3** **11.2.0.4 …**

Oracle **component** where the vulnerability is. Often is Core RDBMS or Network Layer.

Even though the component may not be installed, your database may still be vulnerable.

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-3137	**Oracle RDBMS**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
10.0	**Network**	**Low**	**None**	**Complete**	**Complete**	**Complete**	**10.2.0.3** **10.2.0.4** **10.2.0.5** **…**

The network protocol required to connect in order to exploit the vulnerability. **Oracle Net** (TNS), **Local**, or **HTTP**.

- Oracle Net = connection via SQL*Net
- Local = operating system login such as oracle
- HTTP = web component such as APEX or OEM

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-5858	**Core RDBMS**	**Oracle Net**	**Create Session, Create View**	**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**	**11.1.0.7** **11.2.0.3** **11.2.0.4**

The most important value – tells what privileges are required to exploit the bug. Tells you if it is in a public package (Create Session only), the name the package in some cases, etc.

In this case, requires a valid database session and Create View.

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-1554	**Network Layer**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.0	**Network**	**Low**	**None**	**None**	**None**	**Partial+**	**10.2.0.4** **10.2.0.5** **11.1.0.7 ...**

Is the vulnerability remotely exploitable **without Authentication**? Yes or No. Do I need a valid database session?

Yes = If Oracle Net protocol, then most likely a TNS Listener bug. Very few bugs non-Listener bugs fit this category.
No = Requires a valid database session

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-1554	**Network Layer**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.0	**Network**	**Low**	**None**	**None**	**None**	**Partial+**	**10.2.0.4** **10.2.0.5** **11.1.0.7 ...**

CVSS = Common Vulnerability Scoring System – standard scoring system for security vulnerabilities on a scale of 1.0 to 10.0.

Oracle CVSS are usually in range of 4.0 to 7.0 with 6.5+ being bad. Will see higher scores for Windows vulnerabilities (often 10.0).

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-1554	**Network Layer**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.0	**Network**	**Low**	**None**	**None**	**None**	**Partial+**	**10.2.0.4** **10.2.0.5** **11.1.0.7 ...**

Can the vulnerability be exploited via the **Network** or requires a **Local** operating system login. Most Oracle vulnerabilities are **Network**.

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-1554	**Network Layer**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.0	**Network**	**Low**	**None**	**None**	**None**	**Partial+**	**10.2.0.4** **10.2.0.5** **11.1.0.7 ...**

Confidentiality	Attacker can read data – permission issues, SQL injection, cross-site scripting (XSS), etc.
Integrity	Attacker can write data – SQL injection, buffer overflows, permissions, etc.
Availability	Attacker can bring down the database – denial of service

Reading the CPU Advisory

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2013-1554	**Network Layer**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
5.0	**Network**	**Low**	**None**	**None**	**None**	**Partial+**	**10.2.0.4** **10.2.0.5** **11.1.0.7 ...**

Complete	Your server is completely compromised on Windows
Partial+	Your database is completely compromised on all OS's
Partial	Attacker can get to something but not everything

Oracle Database Vulnerability Breakdown

~40% SQL Injection

~20% Buffer Overflow

~10% Privilege or Permission Issue

~30% Other

Total Vulnerabilities = 433

19%

of bugs exploitable

WITHOUT AUTHENTICATION

53%

of bugs exploitable in

PUBLIC packages

44%

of bugs with

PUBLISHED exploits

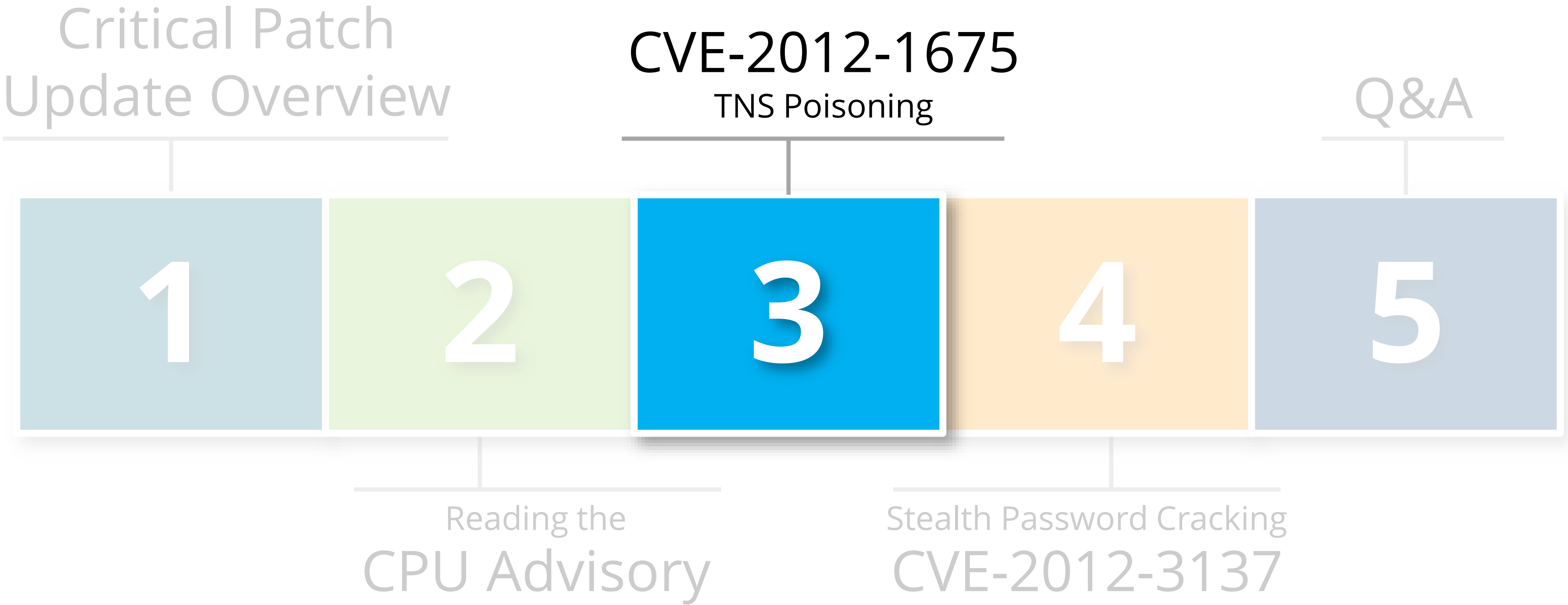
in **PUBLIC** packages

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 Overview

Reading the CPU Advisory

CVE-2012-1675
TNS Poisoning

Stealth Password Cracking
CVE-2012-3137

Q&A

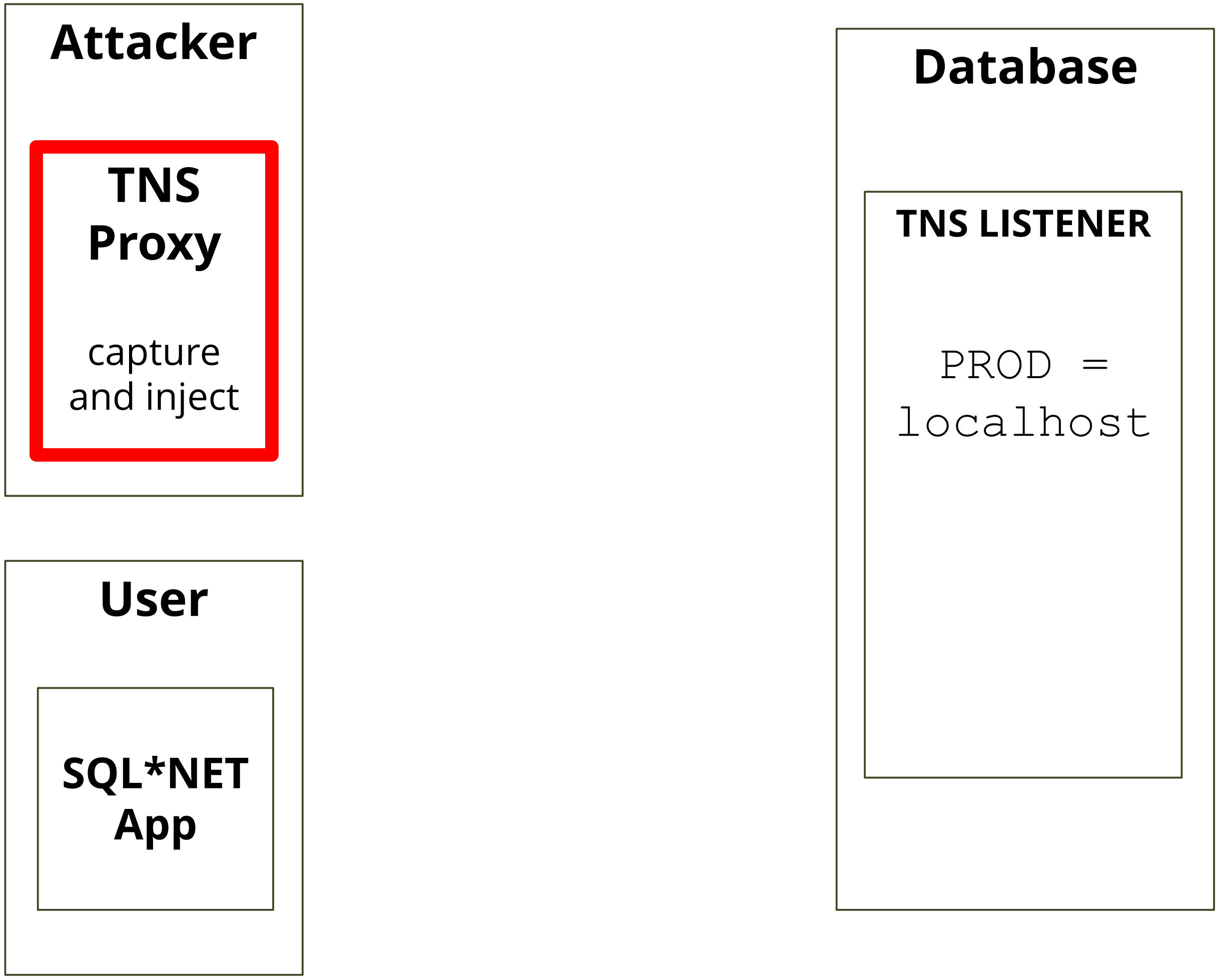
TNS Poisoning Attack – One-off – April 30, 2012

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-1675	**Listener**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
7.5	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**Partial**	**ALL VERSIONS**

- **This vulnerability is not patched by a SPU or PSU.** The TNS Listener configuration must be secured.
- **ALL VERSIONS** of the Oracle Database are affected.
- 12c and 11.2.0.4 protected by default, but vulnerable when Valid Node Checking Registration (VNCR) is disabled.

TNS Poisoning Attack Illustrated



Attacker

TNS Proxy

capture and inject

User

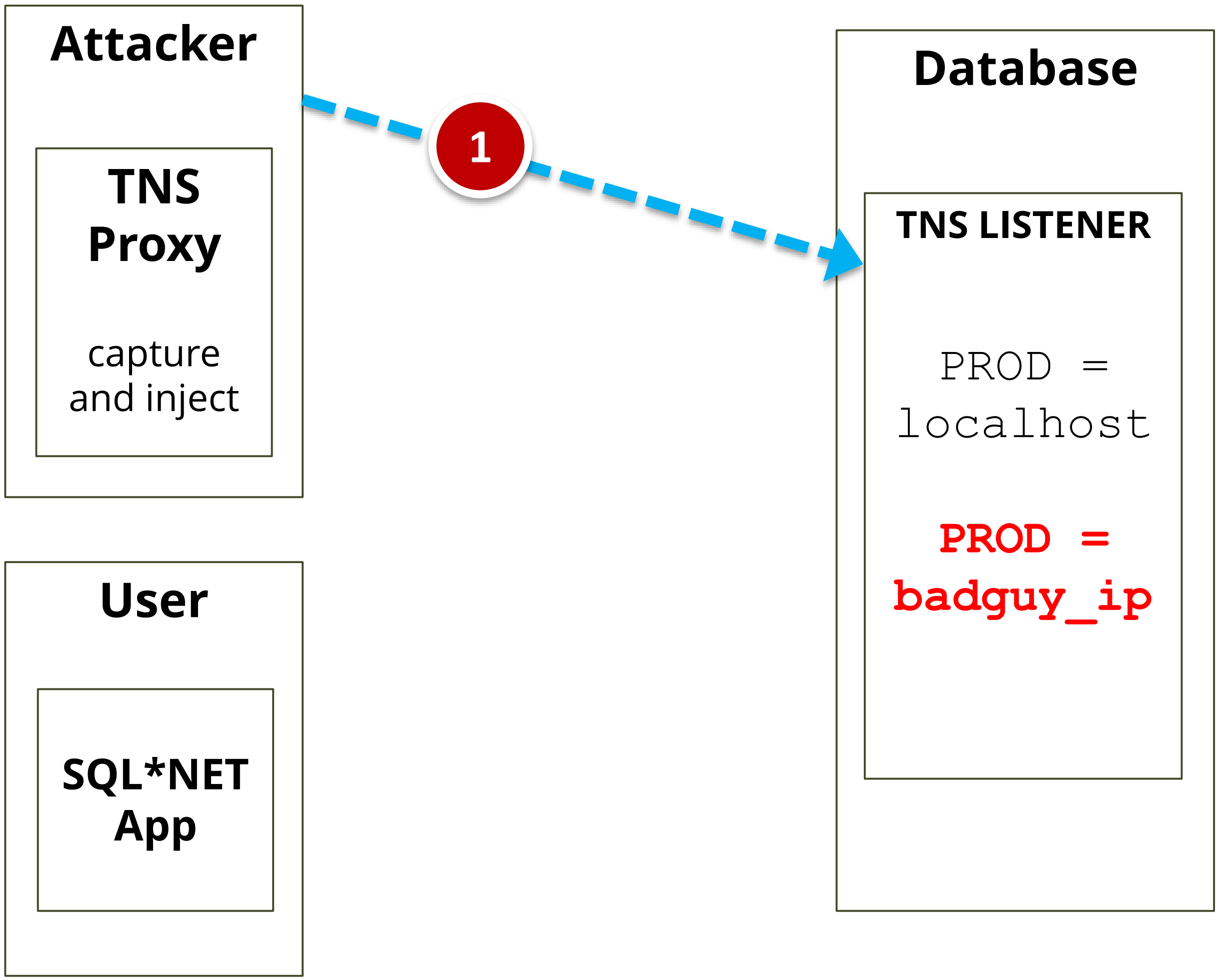
SQL*NET App

Database

TNS LISTENER

PROD = localhost

TNS Poisoning Attack Illustrated



Attacker

TNS Proxy

capture and inject

1

Database

TNS LISTENER

PROD = localhost

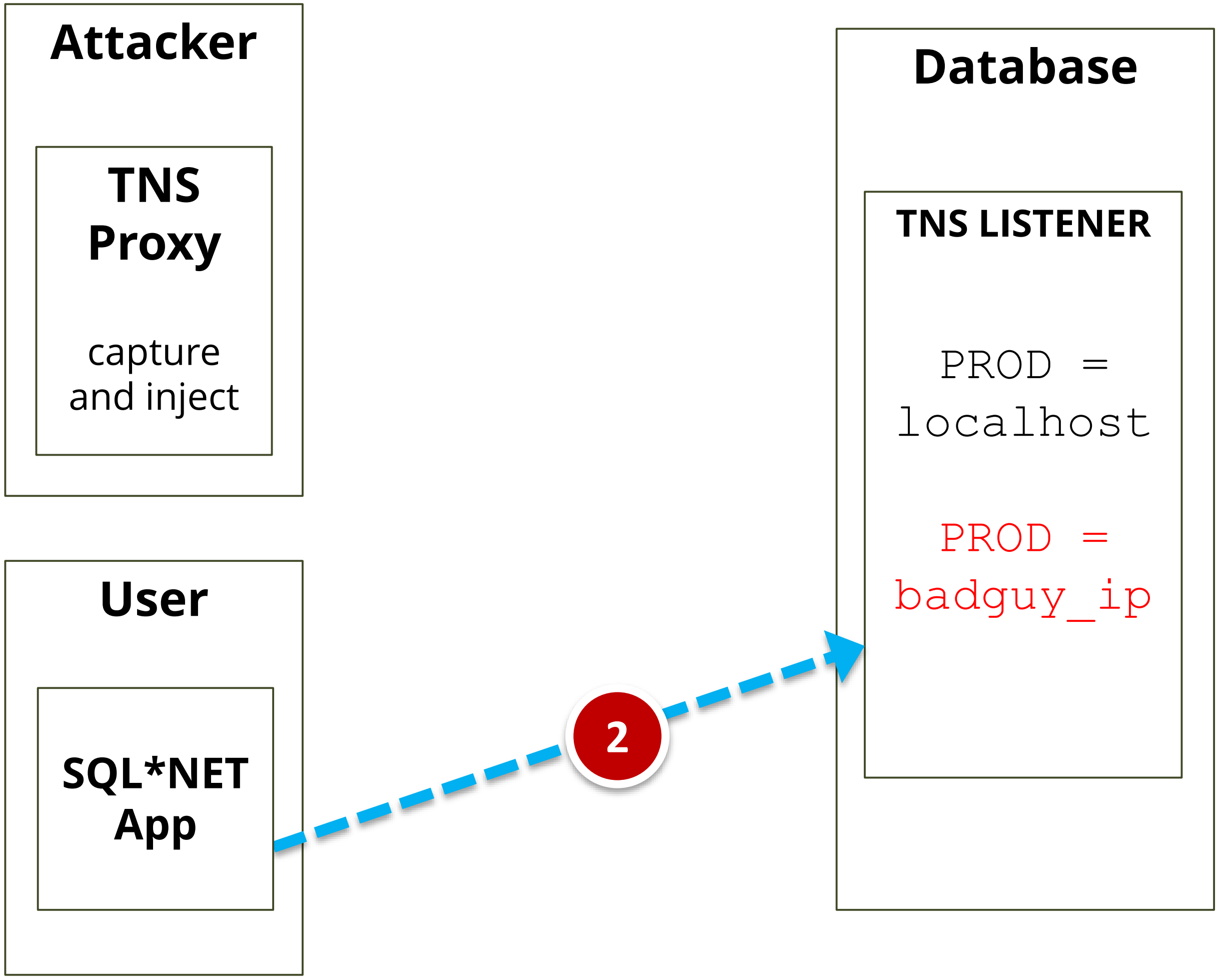
PROD = badguy_ip

User

SQL*NET App

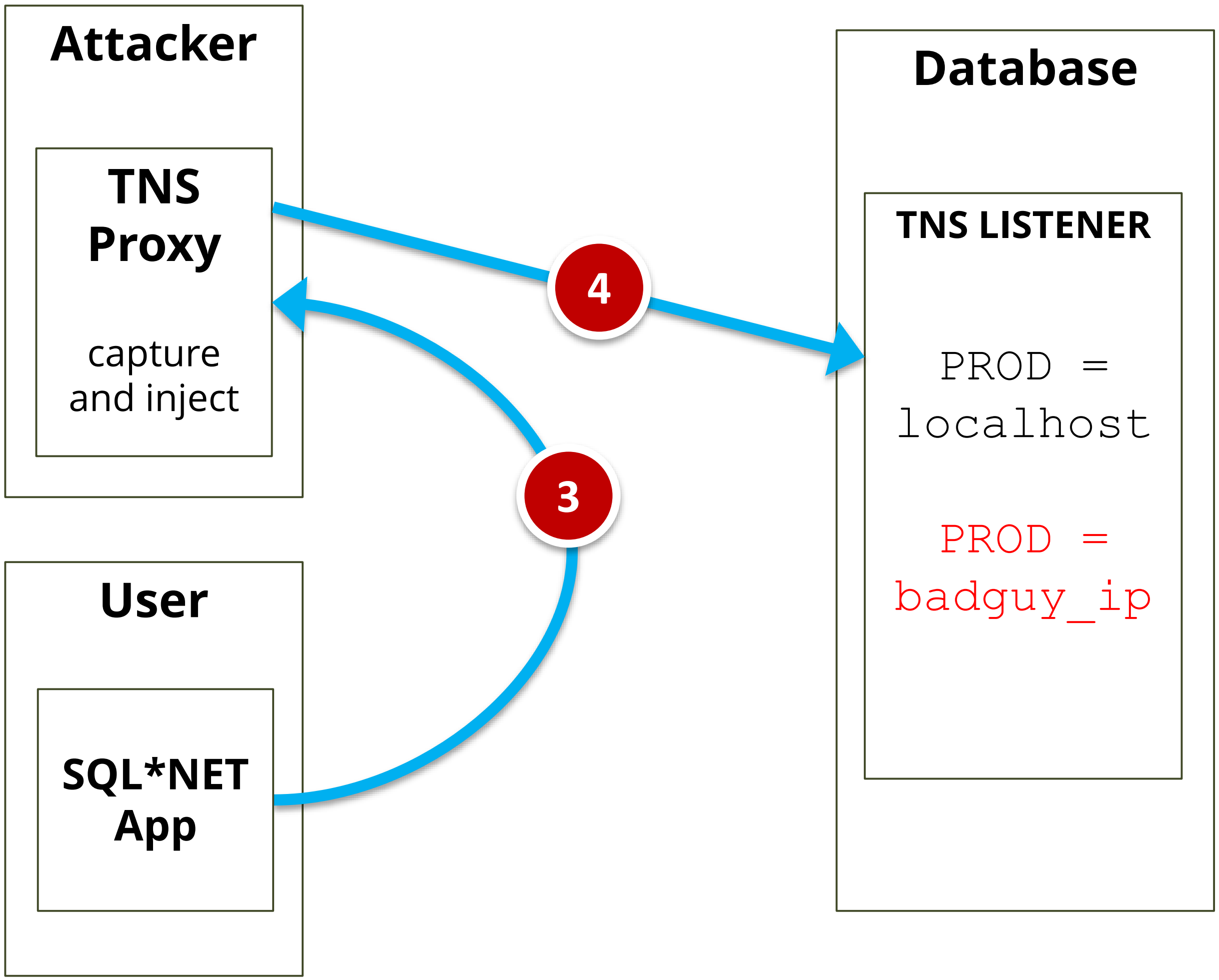
1 Attacker dynamically registers Service with database.

TNS Poisoning Attack Illustrated



2 User connects and is “Load Balanced” to attacker.

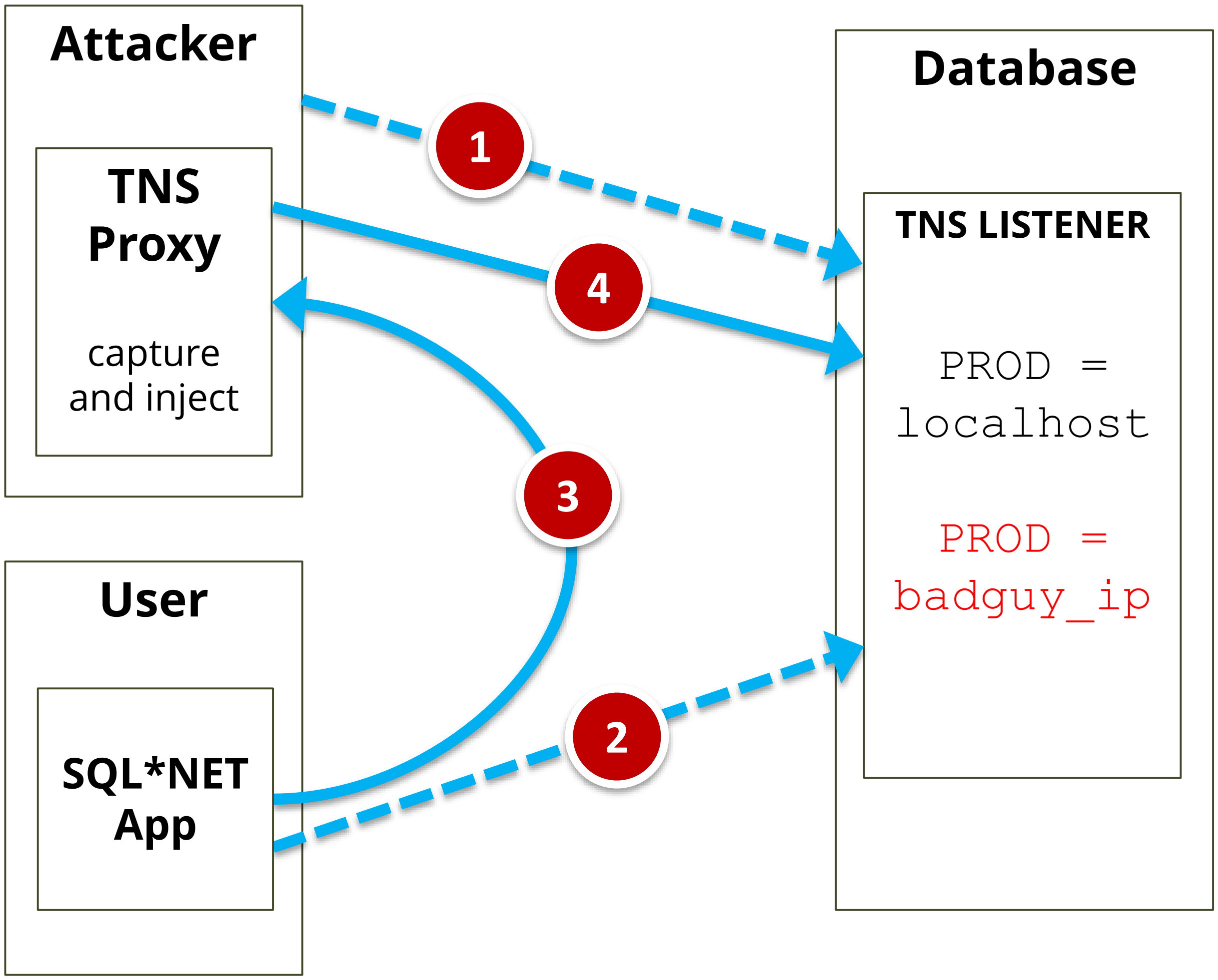
TNS Poisoning Attack Illustrated



3 User connect to attacker rather than database.

4 Attacker forwards to database.

TNS Poisoning Attack Illustrated



1. Attacker dynamically registers Service with database.
2. User connects and is “Load Balanced” to attacker.
3. User connect to attacker rather than database.
4. Attacker forwards to database.

TNS Poisoning Mitigation

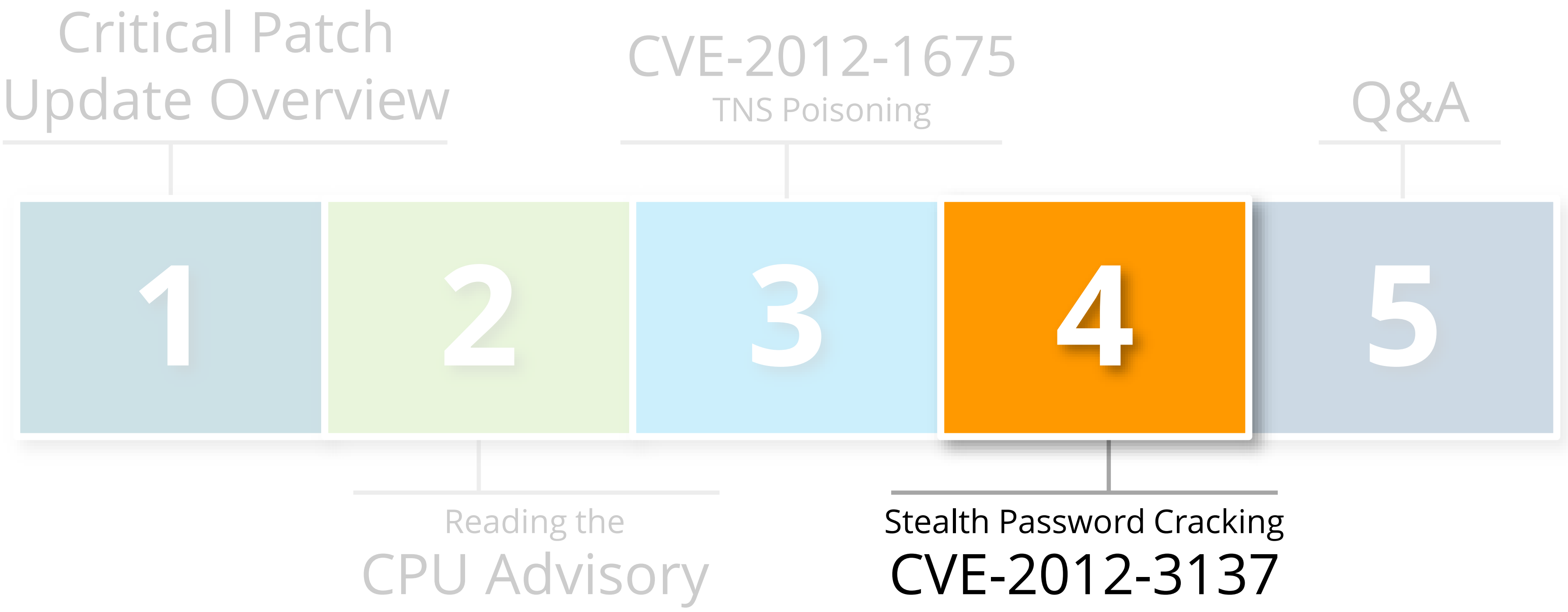
Database Version	***SSL Encrypt with Cert***	***COST*** *class of secure transport*	***VNCR*** *Valid node checking registration*
References	See ASO	1453883.1 1340831.1 (RAC)	1600630.1
8.1.7.x – 10.2.0.3	✓		
10.2.0.3 – 10.2.0.5	✓	✓	
11.1.0.x	✓	✓	
11.2.0.1 – 11.2.0.3	✓	✓	
11.2.0.4*	✓	✓	✓ (Enabled by default)
12.1.0.x*	✓	✓	✓ (Enabled by default)

* 11.2.0.4 and 12c does not allow remote registration by default.

Exploit Information

- **Joxean Koret**
  - http://joxeankoret.com/research.html
  - Oracle TNS Poison un-auth proof on concept (Oracle 9i, 10g and 11g)
- **tnspoisonv1.py**
  - Used to poison the remote database listener
- **proxy.py**
  - Proxy on attacker machine to accept client connections and forward to database server

Agenda



1 Critical Patch Update Overview

2 Reading the CPU Advisory

3 CVE-2012-1675 TNS Poisoning

4 Stealth Password Cracking CVE-2012-3137

5 Q&A

Stealth Password Cracking Bug – October 2012

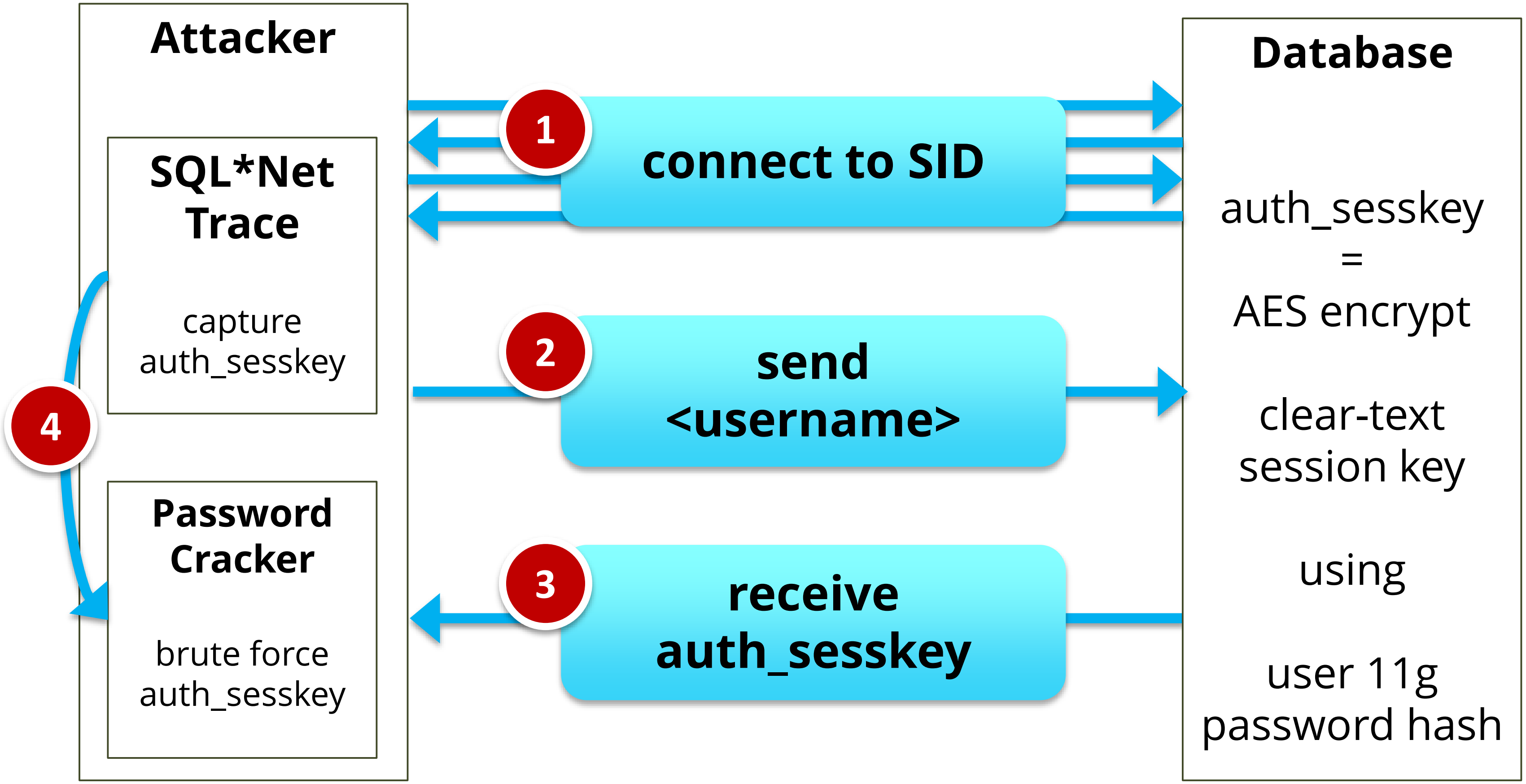
Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2012-3137	**Oracle RDBMS**	**Oracle Net**	**None**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
10.0	**Network**	**Low**	**None**	**Complete**	**Complete**	**Complete**	**11.1.0.x** **11.2.0.1** **11.2.0.2** **11.2.0.3**

Vulnerable if using "11G" passwords (see USER$). 10.2.0.x is also vulnerable if using Enterprise User Security (EUS) with an SHA-1 password verifier.

Stealth Password Attack Illustrated

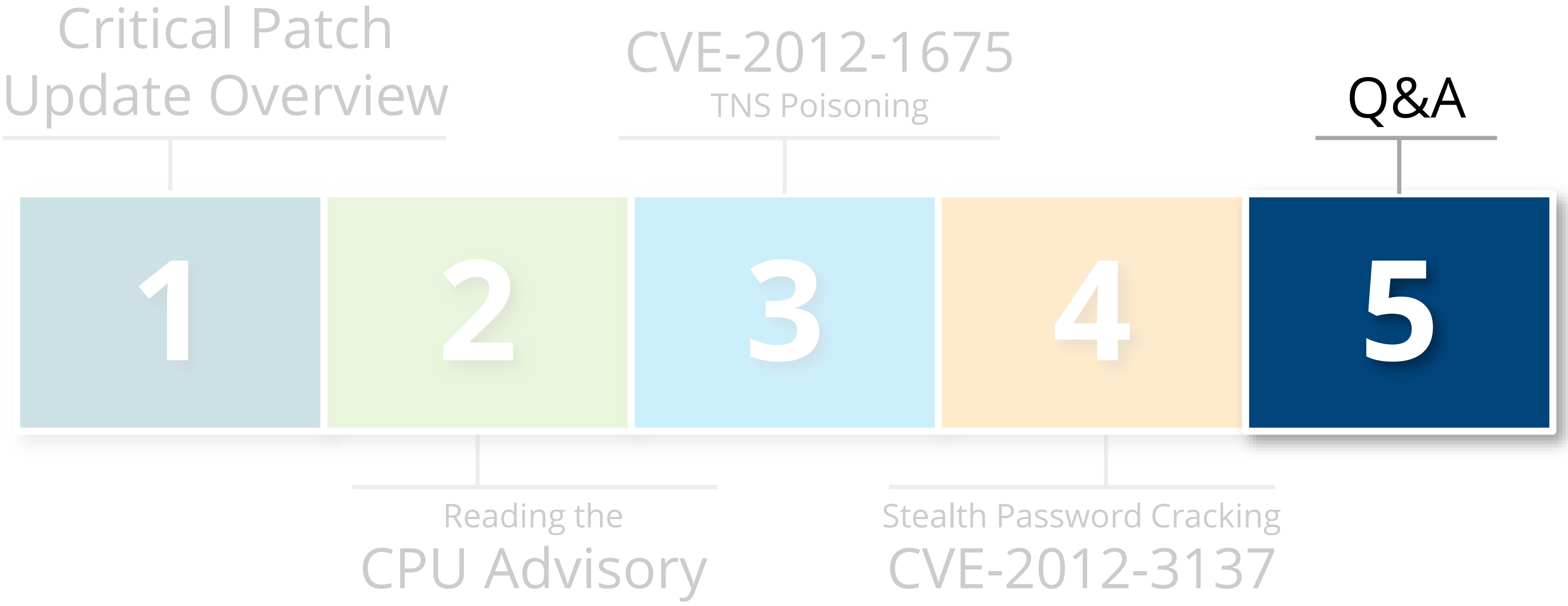
Flaw in the 11g O5Logon protocol allows for brute forcing of the password using the authsess_key.



Exploit Information

- **SQL*Net Trace on client**
  - Capture SQL*Net connection and auth_sesskey
  - TRACE_LEVEL_CLIENT = SUPPORT
- **nmap**
  - Legendary network scanning tool
  - oracle-brute-stealth script
  - Retrieves auth_sesskey for selected users
- **John the Ripper**
  - Legendary password cracking tool
  - Use o5logon

Agenda



Critical Patch Update Overview

Reading the CPU Advisory

CVE-2012-1675
TNS Poisoning

Stealth Password Cracking
CVE-2012-3137

Q&A

Bonus

“Heartbleed”

OpenSSL vulnerability

(CVE-2014-0160)

“CATASTROPHIC”

OpenSSL vulnerability

1.0.1 – 1.0.1f

OpenSSL 1.0.1
released

March 14, 2012

Oracle Impact

Oracle Database – All versions

- Database SSL components (ASO) not vulnerable
- APEX Embed Gateway – most likely not vulnerable

Oracle Application Server 9i (EBS 11.5)

- OpenSSL 0.9.6, 0.9.8 – older versions

Oracle Application Server 10g+ (EBS 12.0/12.1)

- Moved from OpenSSL to mod_ossl to support Oracle Wallet
- Mod_ossl uses older version – OpenSSL 0.9.8 – not vulnerable

Fusion Middleware 11g/12c and WebLogic

- Using mod_ossl and only limited installations of OpenSSL
- Investigating if any versions of mod_ossl are based on OpenSSL 1.0.1
- Investigating if any components use OpenSSL

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**