INTEGRIGY

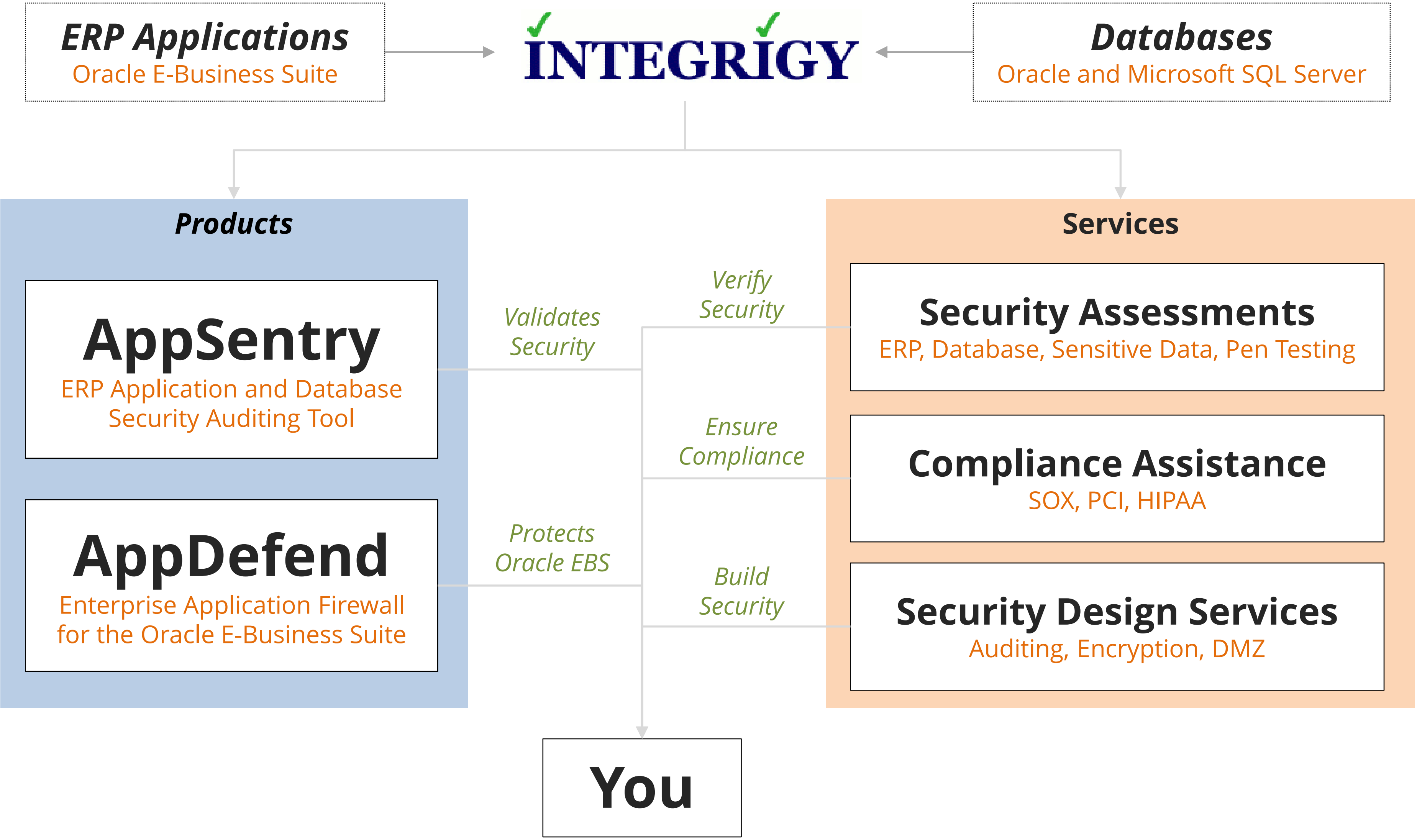
When You Can't Apply Oracle EBS 11i and R12 CPU Security Patches

March 23, 2016

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Why are CPU Patches Not Applied?

Oracle Critical Patch Updates (CPU) are not applied to many Oracle E-Business Suite environments due to support, testing, downtime, and application issues.

- **Lack of IT Management and DBA prioritization of security patches and periodic technical upgrades**

- **Unsupported application or database versions**
  - Oracle EBS 11.5.10 and 12.0 are de-supported for CPUS

- **Dropped Oracle Support or using third-party support**
  - Oracle CPU patches require current Oracle Support

de·sup·port [**dee**-suh-pawrt]

noun

1. the state of not being supported.
2. a phenomenon that occurs to Oracle customers.

verb

1. to end or remove support.

Oracle Product Lifetime Support Model

Premier	▪ Five years from release ▪ Security patches and Critical Patch Updates
Extended	▪ Three years additional ▪ Security patches and Critical Patch Updates ▪ Additional annual fee
Sustaining **(desupport)**	▪ **NO security patches** ▪ **NO Critical Patch Updates** ▪ Indefinite as long as pay annual maintenance ▪ Requires a minimum patch level – usually the terminal patchset or set of patches

Source: http://www.oracle.com/us/support/lifetime-support/index.html

Oracle Software Error Correction Support

Oracle Database Oracle Fusion Middleware Oracle Enterprise Manager	**MOS Note ID 209768.1**
Oracle E-Business Suite	**MOS Note ID 1195034.1**
Oracle Lifetime Support	http://www.oracle.com/us/support/lifetime-support/index.html

Oracle Database Version Support

Major Releases	Extended Support End Date	Patchsets	CPU Support End Date
Oracle 12c R1	July 2021	**12.1.0.2**	**July 2021**
		12.1.0.1	**July 2016** (extended from July 2015)
Oracle 11g R2	December 2020	**11.2.0.4**	**October 2020** (extended from October 2018)
		~~11.2.0.3~~	~~July 2015~~
		~~11.2.0.2~~	~~January 2013~~
		~~11.2.0.1~~	~~July 2011~~
Oracle 11g R1	~~August 2015~~	~~11.1.0.7~~	~~July 2015~~
~~**Oracle 10g R2**~~	~~July 2013~~	~~10.2.0.5~~	~~July 2013~~
~~**Oracle 10g R1**~~	~~January 2012~~	~~10.1.0.5~~	~~January 2012~~

Oracle E-Business Suite Version Support

Version	Premier Support End Date	Extended Support End Date (1)	CPU Support End Date
EBS 12.2	September 2021	TBD	**TBD**
EBS 12.1	December 2016	December 2019	**October 2019**
~~**EBS 12.0**~~	~~January 2012~~	~~January 2015~~	**January 2015**
~~**EBS 11.5.10**~~	~~November 2010~~	~~November 2013~~	**January 2016 (2, 3)**
~~**EBS 11.5.9**~~	~~June 2008~~	~~N/A~~	~~July 2008~~
~~**EBS 11.5.8**~~	~~November 2007~~	~~N/A~~	~~October 2007~~
~~**EBS 11.5.7**~~	~~May 2007~~	~~N/A~~	~~April 2007~~

1. Extended support requires a minimum baseline patch level – see MOS Note ID 1195034.1.
2. After January 2016, CPUs are available for customers with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through January 2016 provides CPUs.

Oracle EBS Extended Support Requirements

12.2	▪ EBS 12.2.3 ▪ R12.AD.C.DELTA.7
12.1	▪ Basically 12.1.3 ▪ Application Server 10.1.3.5
12.0	▪ EBS 12.0.6 ▪ Application Server 10.1.2.3 & 10.1.3.5 ▪ Java 6
11.5.10	▪ ATG RUP 6 or ATG RUP 7

Source: MOS Note ID 1195034.1 - Oracle E-Business Suite Error Correction Support Policy (V.5 – January 2015)

Security Implications of Desupport

1. No security patches or Critical Patch Updates
2. No security configuration updates
3. No technology stack updates or upgrades
4. No major security documentation updates
5. No research or validation of submitted security bugs

No Security Configuration Updates

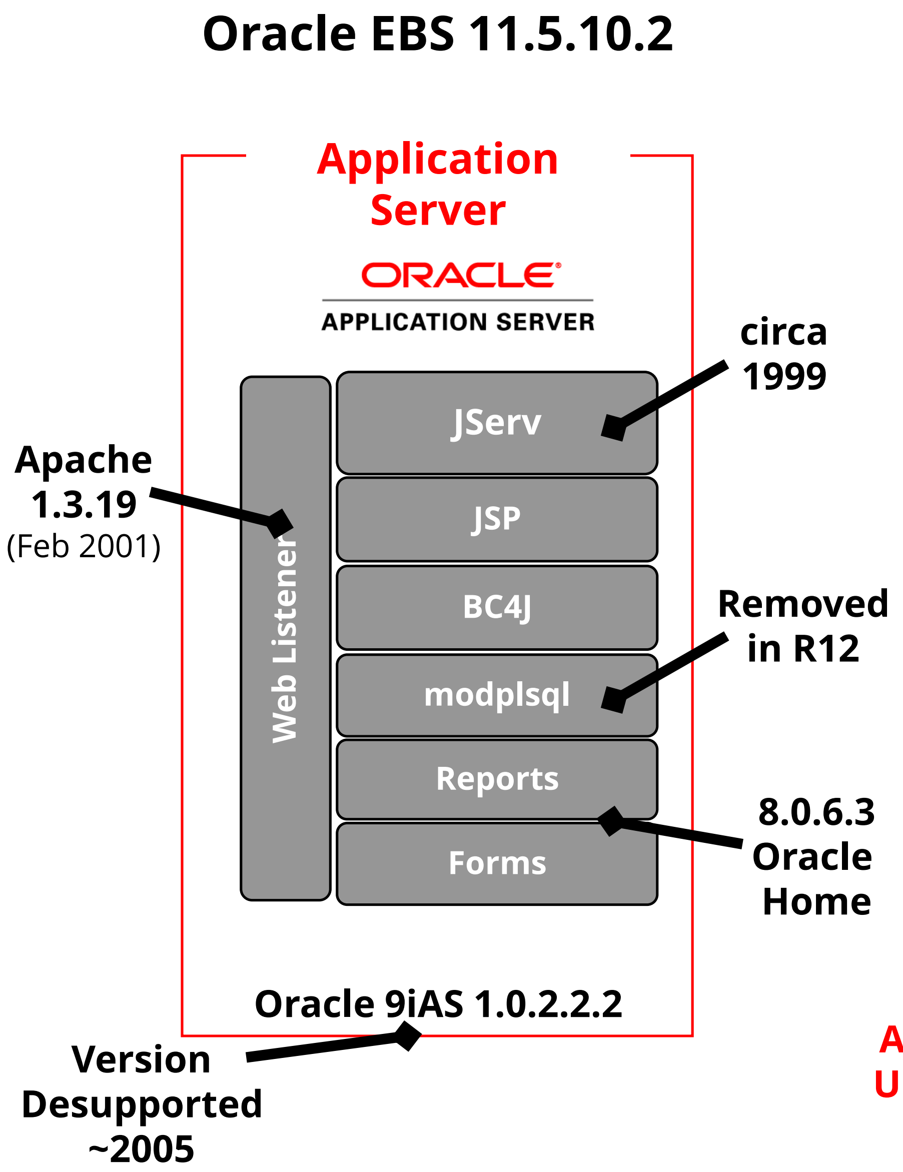
- **State of security changes over time**
  - Hacking techniques and tools evolve
  - HTTP cookie security is a prime example

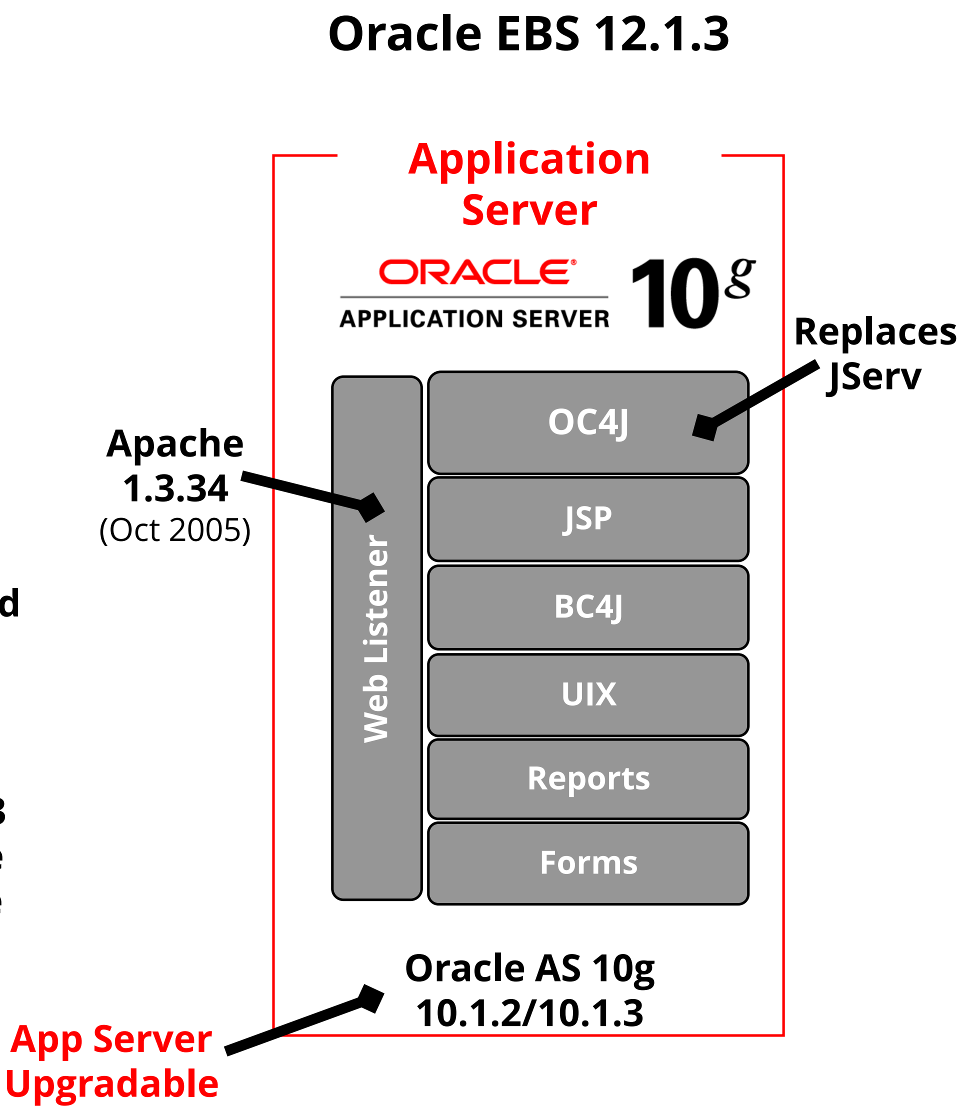
- **Oracle improves security with tweaks to configuration settings through patches and security patches**
  - Mostly minor and behind the scenes changes, but impact security in a meaningful way
  - Oracle Database privilege changes
  - Oracle E-Business Suite web server configuration

No Technology Stack Updates or Upgrades

- **Oracle Database**
  - APEX versions not certified
- **Oracle E-Business Suite**
  - New database versions not certified – no security patches for the database
  - Application server security patches not available
  - Apache, Forms, Reports, JServ, and SSL versions for 11.5.10 are ancient – security improvements as well as patches

11i/R12 Architecture Differences





No Security Documentation Updates

- **Oracle Database**
  - Oracle Security Guide not updated

- **Oracle E-Business Suite**
  - Oracle EBS Security Configuration Guide not updated
    - 11i = MOS Note ID 189367.1
    - Last Update September 2011

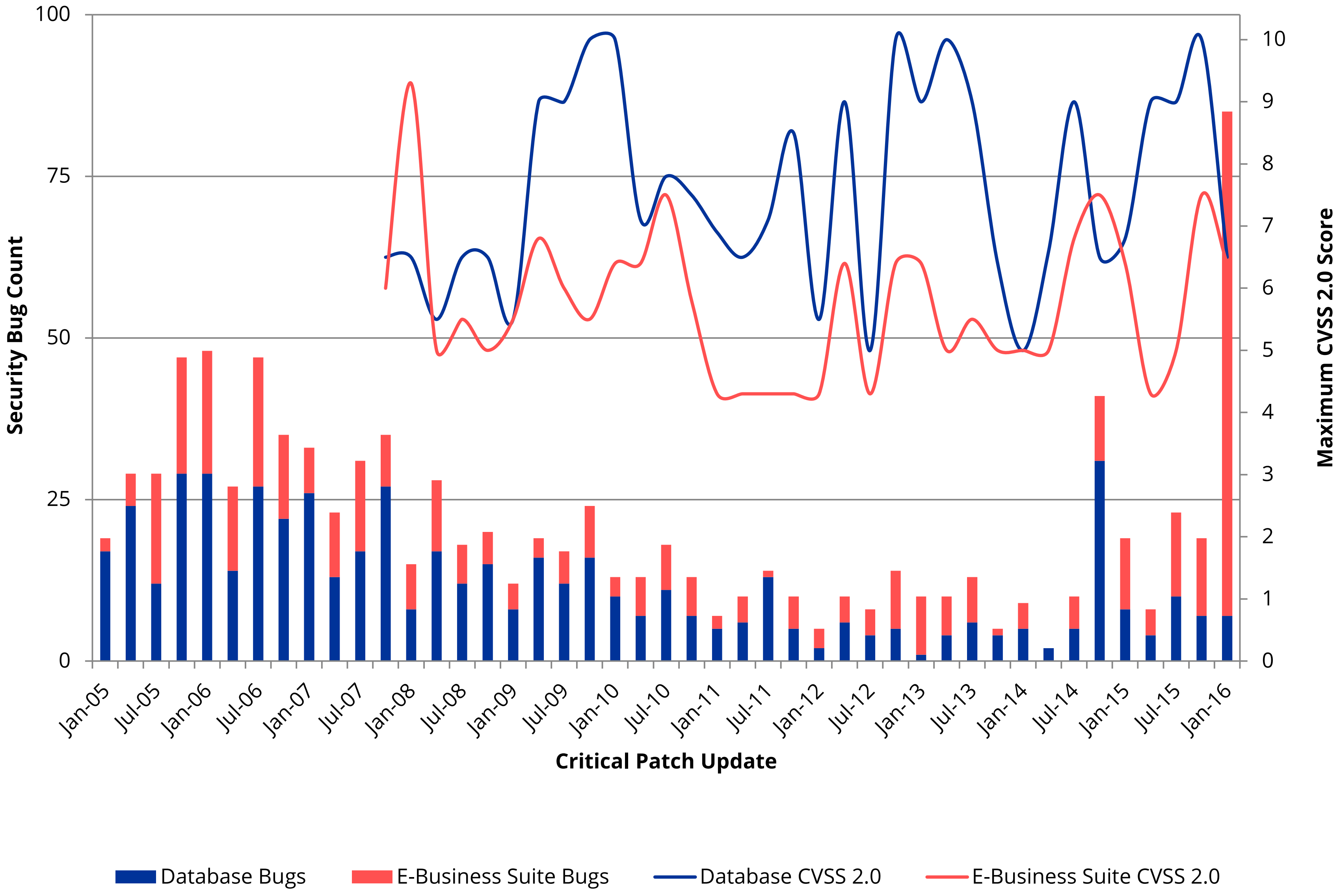
  - Oracle EBS DMZ Configuration not updated
    - 11i = MOS Note ID 287176.1
    - Last Update October 2011

No Security Vulnerability Research

- **Oracle Software Security Assurance stated policy is not to fix security bugs in desupported products**
  - Researched for supported products
  - Fixed in main code-line first
  - Backported to support products

- **Security bugs may be found in desupported version and never validated by Oracle**
  - Unclear what Oracle's reaction would be to a major vulnerability in a desupported product

Oracle Security Vulnerabilities per Quarter



Oracle E-Business Suite Critical Patch Updates

Oracle EBS CPU Risks and Threats

The risk of Oracle E-Business Suite security vulnerabilities depends if the application is externally accessible and if the attacker has a valid application session.

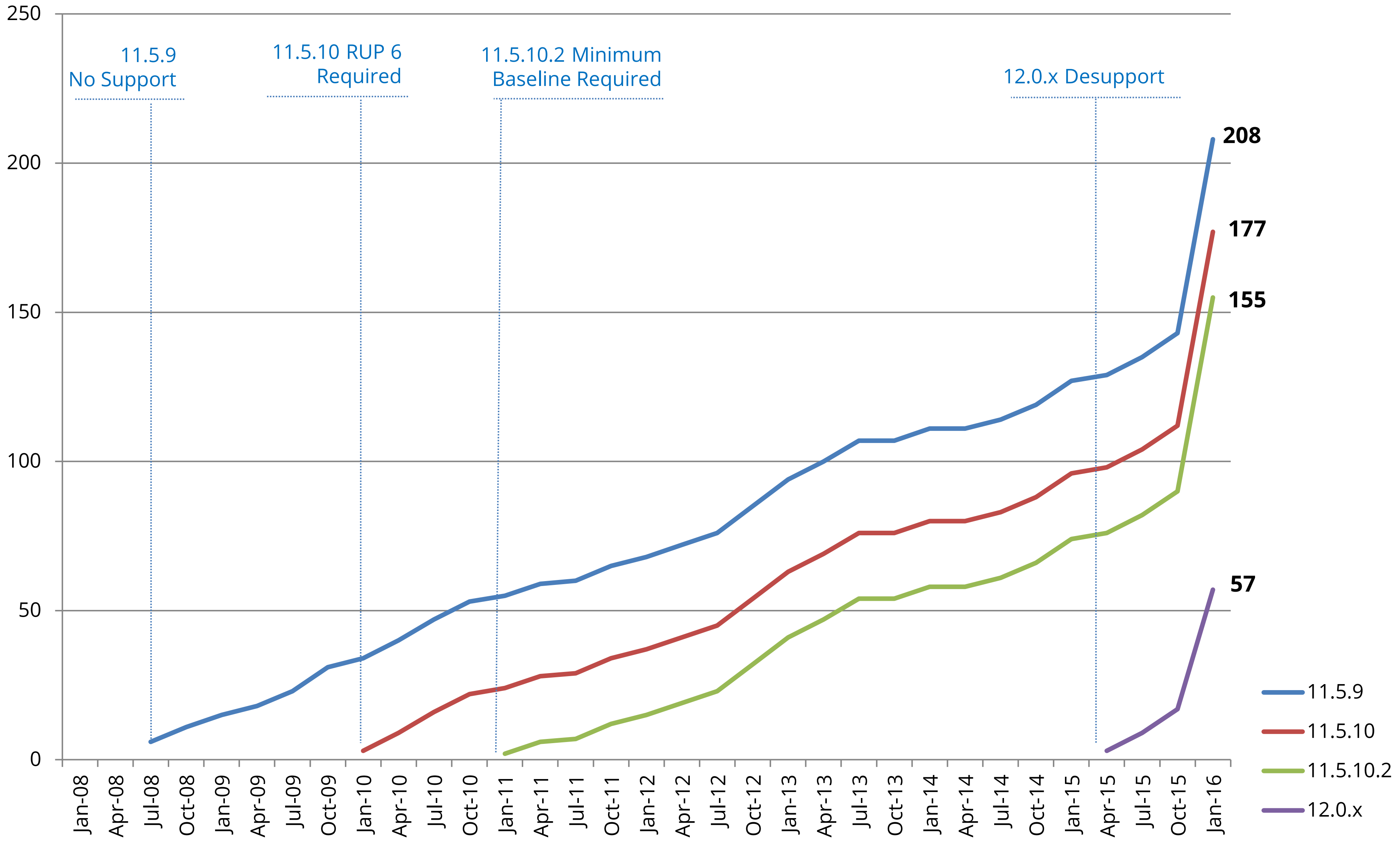
Type of User	Application Session	Description
External/DMZ unauthenticated user	No	Access external URL
External/DMZ authenticated user	Yes	Any responsibility
Internal unauthenticated user	No	Access internal URL
Internal authenticated user	Yes	Any responsibility

Oracle EBS CPU Risks and Threats

The risk of Oracle E-Business Suite security vulnerabilities depends if the application is externally accessible and if the attacker has a valid application session.

Type of User	Application Session	Description
External/DMZ unauthenticated user	No	Access external URL
External/DMZ authenticated user	Yes	Any responsibility
Internal unauthenticated user	No	Access internal URL
Internal authenticated user	Yes	Any responsibility

EBS Cumulative Vulnerabilities per Version



11.5.10.2 CPU Risk Mapping Example

Type of User	**Number of Security Bugs**	**Notes**
External unauthenticated user	21[1]	▪ **17 of 21 are high risk**
External authenticated user	6[1]	▪ 3 of 6 are exploited with only a valid application session
Internal unauthenticated user	17	▪ **Many are high risk**
Internal authenticated user	10	▪ Most require access to specific module in order to exploit

[1] Assumes URL firewall is enabled and count is for all external “i” modules (iSupplier, iStore, etc.).

Solutions by Risk for No CPUs

Type of User	Solutions if CPUs not applied
External unauthenticated user	#1 – Enable Oracle EBS URL firewall #2 – Implement Integrigy's AppDefend
External authenticated user	#3 – Enable Oracle EBS external responsibilities
Internal unauthenticated user	#4 – Implement Integrigy's AppDefend
Internal authenticated user	#5 – Limit access to privileged responsibilities

Integrigy AppDefend for Oracle EBS

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite.

- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and Oracle EBS security risks

- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules

- **Virtual Patching**
  Detects and blocks known Oracle EBS security vulnerabilities

- **Application Logging**
  Enhanced application logging for compliance requirements like PCI-DSS 10.2

OWASP Top 10 – AppDefend

AppDefend

A1: Injection

AppDefend

A2: Cross Site Scripting (XSS)

A3: Broken Authentication and Session Management

AppDefend

A4: Insecure Direct Object References

AppDefend

A5: Cross Site Request Forgery (CRSF)

AppDefend

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

AppDefend

A8: Failure to Restrict URL Access

AppDefend

A9: Insufficient Transport Layer Protection

AppDefend

A10: Unvalidated Redirects and Forwards

High Risk

Medium Risk

Low Risk

OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

Oracle EBS DMZ MOS Notes

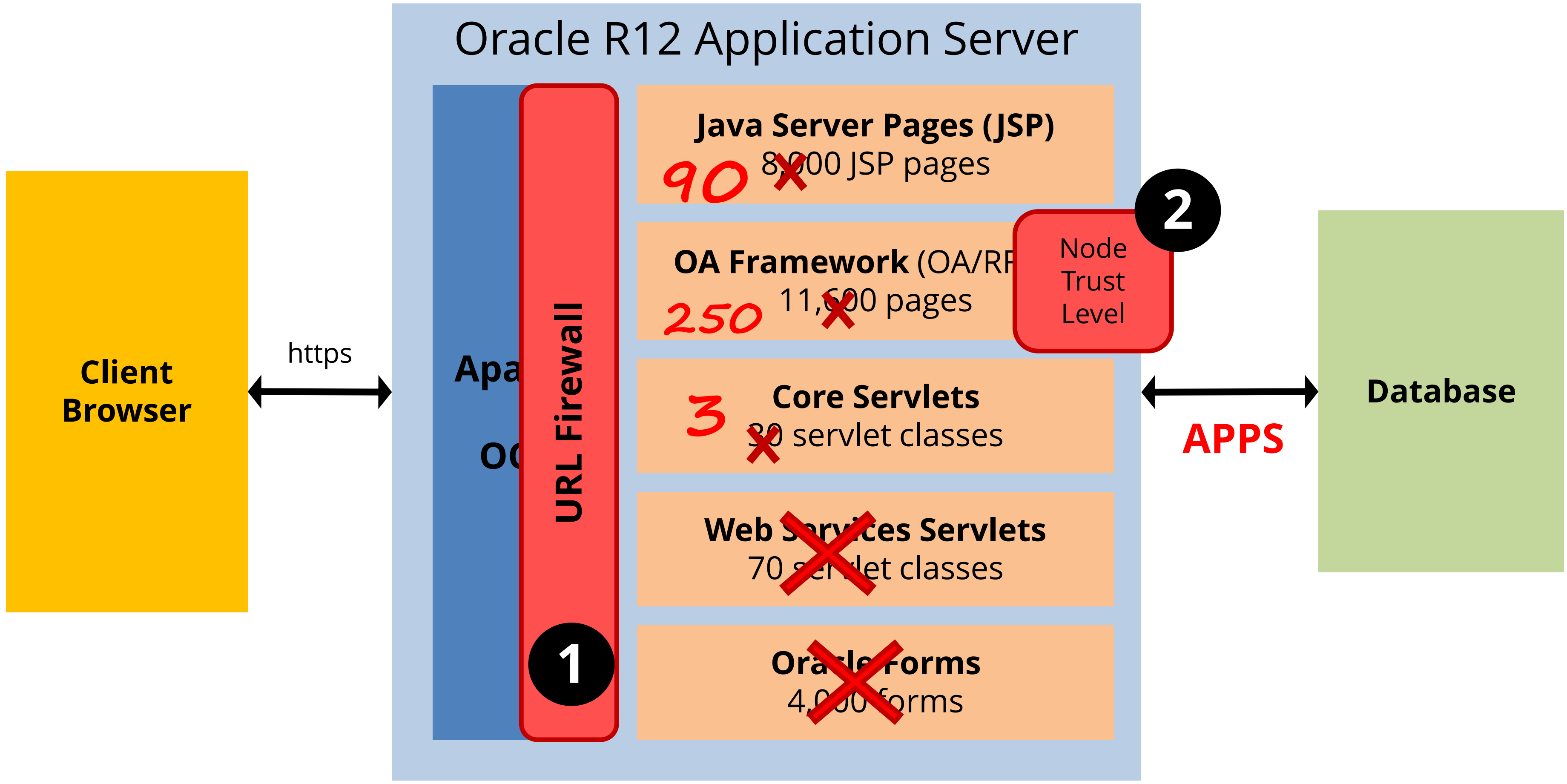
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided MOS Note must be followed.

380490.1 *Oracle E-Business Suite* ***R12*** *Configuration in a DMZ*

287176.1 *DMZ Configuration with Oracle E-Business Suite* ***11i***

MOS = My Oracle Support

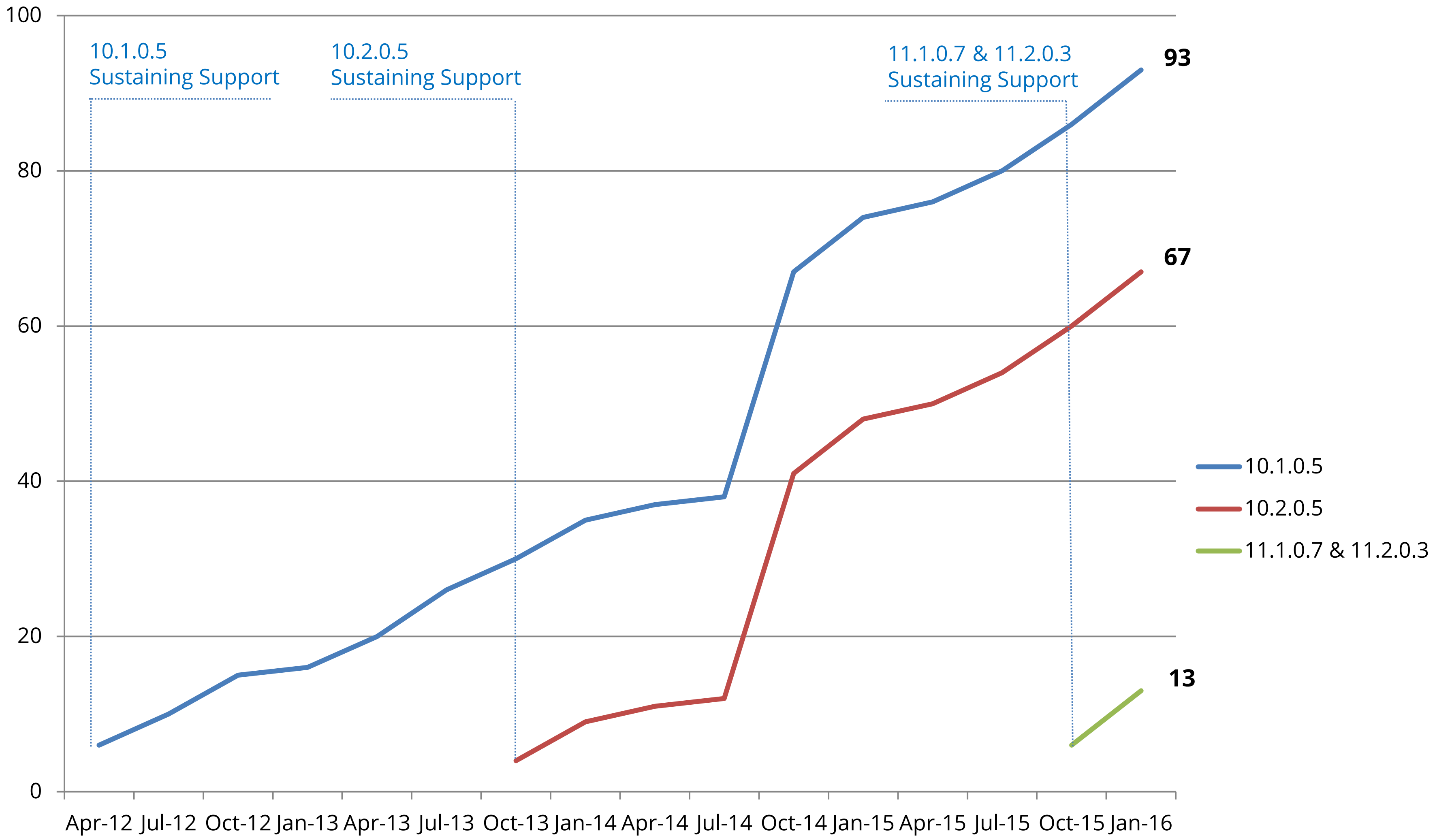
Oracle EBS DMZ Configuration



- Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.

Oracle Database
Critical Patch Updates

Cumulative Vulnerabilities per DB Version



Cumulative maximum count of open security vulnerabilities assuming no security patches have been applied since the start of Extended Support

Oracle Database CPU Risks and Threats

The risk of Oracle database security vulnerabilities depends if an attacker has a database account or can obtain a database account.

Type of User	Database Account	Description
Unauthenticated user	No	Can connect to database listener if IP address, port, SID is known
Low privileged user	Yes	Only PUBLIC privileges
Moderate privileged user	Yes	Some privileges
High privileged user	Yes	DBA like privileges

11.2.0.2 CPU Risk Mapping Example

Type of User	Number of Security Bugs	Notes
Unauthenticated user No database account	9	**1 – O5LOGON Authentication** 7 – Denial of service
Low privileged user Create session system privilege only	7	▪ **Averages one per CPU** ▪ **Requires only PUBLIC privileges**
Moderate privileged user Create table, procedure, index, etc.	6	▪ Usually requires CREATE PROCEDURE system privilege
High privileged user DBA, SYSDBA, local OS access, etc.	7	2 – SYSDBA privileges 3 – Advanced privileges 2 – Local OS access

Solutions by Risk for No CPUs

Type of User	**Solutions if CPUs not applied**
Unauthenticated user No database account	**#1 – Limit direct access to the database** #2 – Check for default passwords #3 – Use only named accounts #4 – No generic read-only accounts
Low privileged user Create session system privilege only	
Moderate privileged user Create table, procedure, index, etc.	#5 – Limit privileges in production
High privileged user DBA, SYSDBA, local OS access, etc.	#6 – External database auditing solution #7 – Limit OS access for prod to DBAs #8 – Use Oracle Database Vault

Limit Database Access

1. **Enterprise firewall and VPN solutions**
    - Block all direct database access outside of the data center
2. **SQL*Net Valid Node Checking**
    - Included with database
    - Block access by IP address
3. **Oracle Connection Manager**
    - SQL*Net proxy server, included with database
    - Block access by IP address or range
4. **Oracle Database Firewall**
    - Add-on database security product

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**