INTEGRIGY

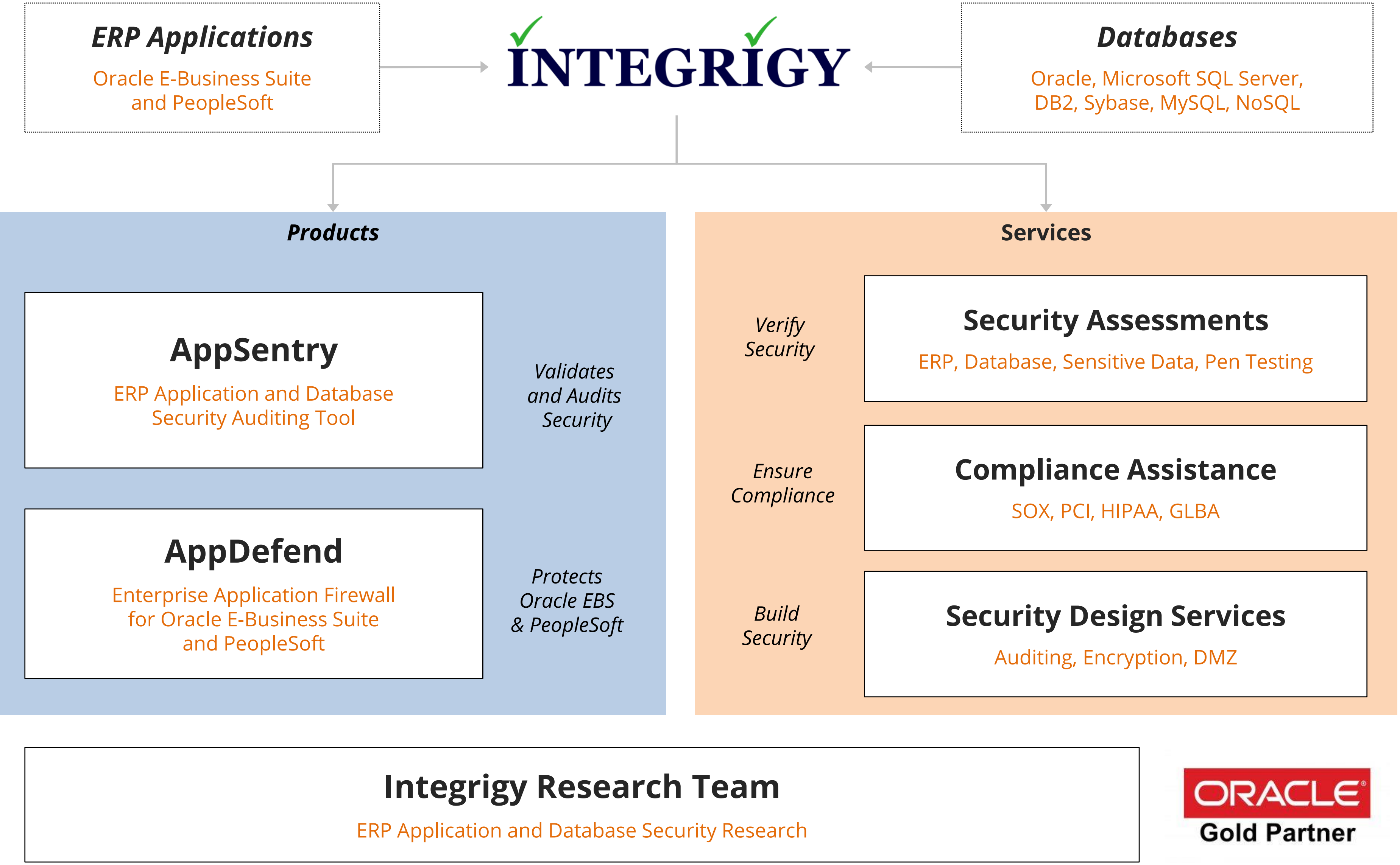
Security Implications of Oracle E-Business Suite 12.1.3 End of Support

May 20, 2021

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications

Oracle E-Business Suite
and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates and Audits Security

AppDefend

Enterprise Application Firewall for Oracle E-Business Suite and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE
Gold Partner

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 Critical Patch Updates = No security patches** ▪ Indefinite as long as you 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 PeopleSoft	MOS Note ID 1560835.1
Oracle Lifetime Support	http://www.oracle.com/us/support/lifetime-support/index.html

Oracle E-Business Suite Version Support

Version	Premier Support End Date	Extended Support End Date	CPU Support End Date
EBS 12.2	**December 2032**	n/a	**TBD**
EBS 12.1	December 2021	n/a	**October 2021 (1)**
EBS 12.0	January 2012	January 2015	January 2015
EBS 11.5.10	November 2010	November 2013	January 2016 (2, 3)

1. After October 2021, CPUs are available with Market Driven Support for 2022 and 2023.
2. After January 2016, CPUs are available with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through January 2016 provides CPUs.

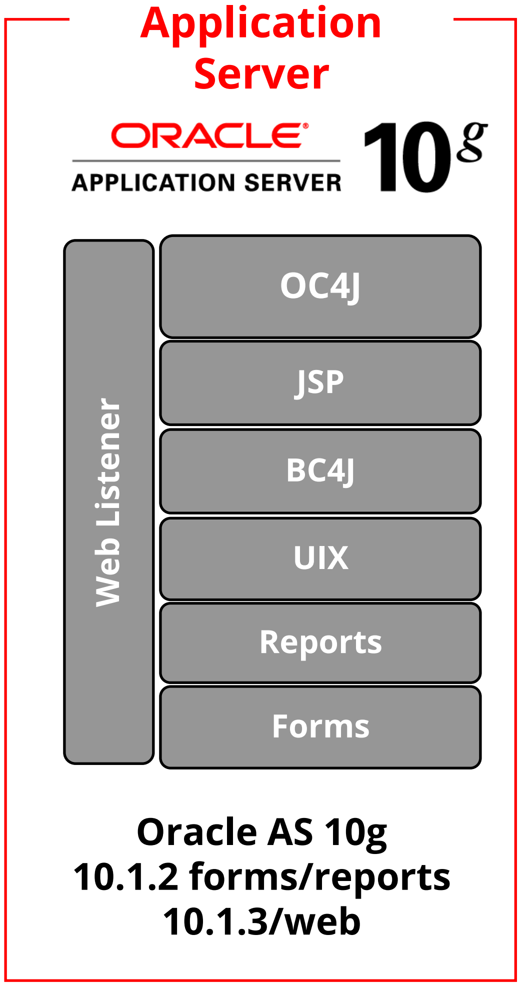
Oracle EBS 12.1.3 Technology Stack

Component	Versions	Extended Support
Database	19c	April 2027
	12.1.0.2	July 2022
	12.1.0.1	July 2016
	11.2.0.4	**October 2020 (3)**
	11.2.0.1-3	July 2015
	10.2.0.x	July 2013
Application Server	10.1.3.x (web)	June 2017 (2)
	10.1.2.x (forms)	December 2011 (2)
Java (server)	1.7 (1)	July 2022
	1.6	October 2017

1. Public updates ended July 2015.
2. Oracle EBS exception with as necessary CPUs – 10.1.3 last CPU as October 2015.
3. 11.2.0.4 support after October 2020 available through Market Driven Support.

Oracle EBS 12.1.3 Application Server Architecture

Oracle EBS 12.1.3



Component	Version	Release Date
AS 10g (Web)	10.1.3.5.1	November 2009
AS 10g (Forms)	10.1.2	December 2005
OHS Apache	1.3.34	October 2005
Oracle OC4J	10.1.3	November 2009
Oracle JSP	10.1.3	November 2009
Oracle Forms	10.1.2	December 2005
Oracle Reports	10.1.2	December 2005

Oracle EBS Minimum Support Requirements for Patching

12.2	▪ EBS 12.2.3 ▪ R12.AD.C.DELTA.5 ▪ R12.TXK.C.DELTA.5
12.1	▪ Basically 12.1.3 ▪ Application Server 10.1.3.5 ▪ R12.ATG_PF.B.DELTA.3 ▪ R12.TXK.B.DELTA.3
12.0	▪ EBS 12.0.6 ▪ Application Server 10.1.2.3 & 10.1.3.5 ▪ Java 6

Source: MOS Note ID 1195034.1 - Oracle E-Business Suite Error Correction Support Policy (V.6 – June 2020)

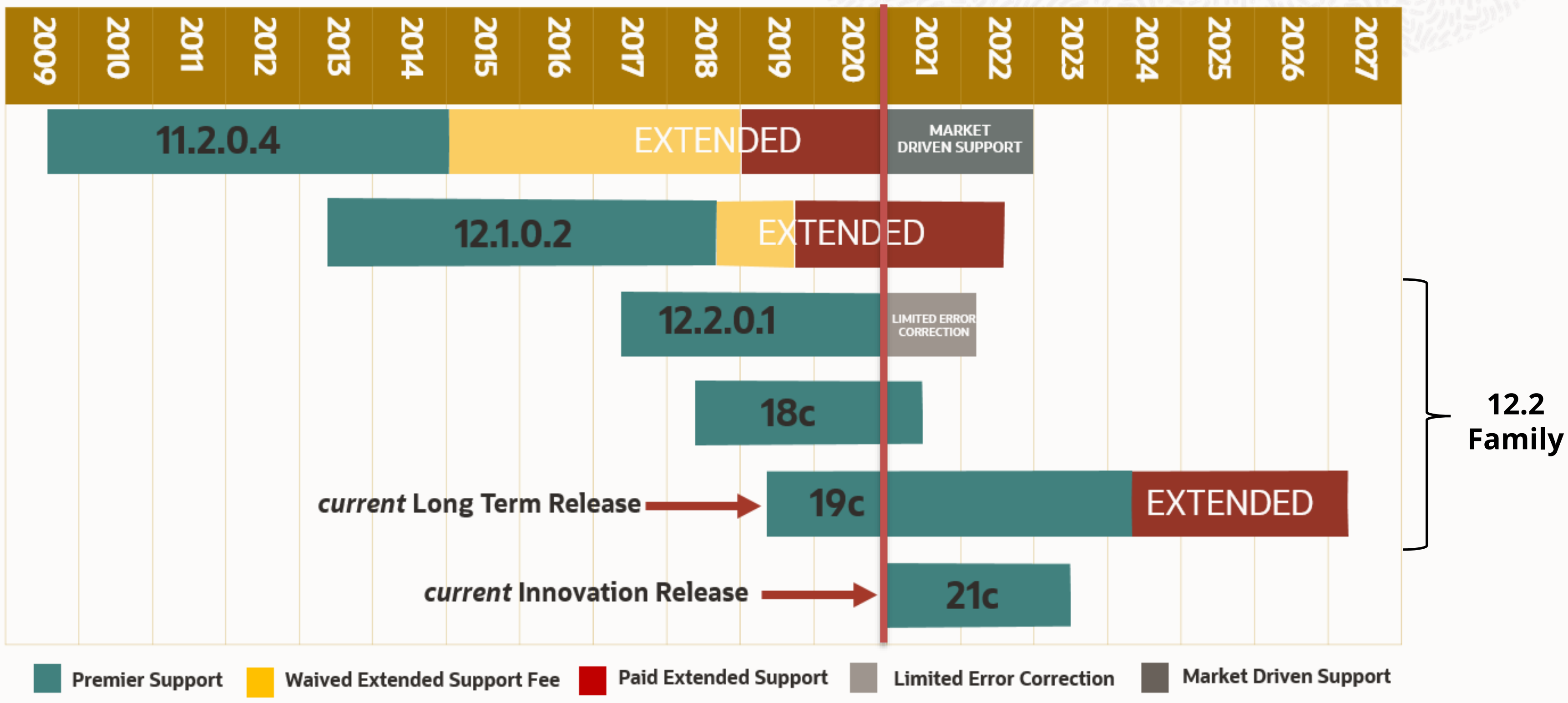
Oracle EBS Database Version Support

Major Releases	Extended Support End Date	Patchsets	CPU Support End Date
Oracle 19c	April 2027	**n/a**	**April 2027**
Oracle 12c R1	July 2021	**12.1.0.2**	**July 2022 (1)**
		12.1.0.1	**July 2016**
Oracle 11g R2	December 2020	**11.2.0.4**	**October 2020 (2)**
		11.2.0.3	July 2015
		11.2.0.2	January 2013
		11.2.0.1	July 2011

1. 12.1.0.2 = Support for EBS extended to July 2022 without fees, see MOS ID 2522948.1.
2. 11.2.0.4 = Market driven support available for 2021 and 2022, see MOS ID 2728619.1.
3. See MOS ID 742060.1 *Release Schedule of Current Database Releases*.

Oracle Database Releases

Database Releases and Support Timelines



Source – Oracle Database (RDBMS) Releases Support Status Summary (Doc ID 161818.1) – January 15, 2021

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
  - 11.5.10 = Apache, Forms, Reports, JServ, and SSL versions are ancient – security improvements as well as patches

No Security Documentation Updates

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

- **Oracle E-Business Suite**
  - Oracle EBS Security Configuration Guide not updated
    - 12.1 = MOS Note ID 403537.1
    - Last Update October 2020
  - Oracle EBS DMZ Configuration not updated
    - 12.1 = MOS Note ID 380490.1
    - Last Update July 2020

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 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

12.1.3 CPU Risk Mapping – Missing One Year of CPUs

Type of User	Number of Security Bugs	Notes
External unauthenticated user	18 (1)	▪ 16 of 18 are high risk
External authenticated user	5 (1)	▪ 3 of 5 are exploited with only a valid application session
Internal unauthenticated user	34	▪ Most are high risk
Internal authenticated user	12	▪ 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 Oracle E-Business Suite CPUs

Type of User	Solutions if CPUs not applied
External unauthenticated user	#1 – Enable Oracle EBS URL firewall for DMZ #2 – Virtual Patching (AppDefend)
External authenticated user	#3 – Enable Oracle EBS external responsibilities
Internal unauthenticated user	#4 – Enabled Allowed Resources (Oct 2020 CPU) #5 – Virtual Patching (AppDefend)
Internal authenticated user	#6 – Limit access to privileged responsibilities

Integrigy AppDefend

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

Prevents Web Attacks

Virtually patches known Oracle EBS vulnerabilities and protects against SQL Injection and XSS

Application Logging

Enhanced application logging for compliance requirements like SOX, GDPR, PCI-DSS 10.2

Two-factor Authentication (2FA)

Enables two-factor authentication for login, user, responsibility, or function

Limits EBS Modules

More flexibility and capabilities than URL firewall to identify EBS modules

Protects Web Services

Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

Protects Mobile Applications

Detects and reacts to attacks against Oracle EBS mobile applications

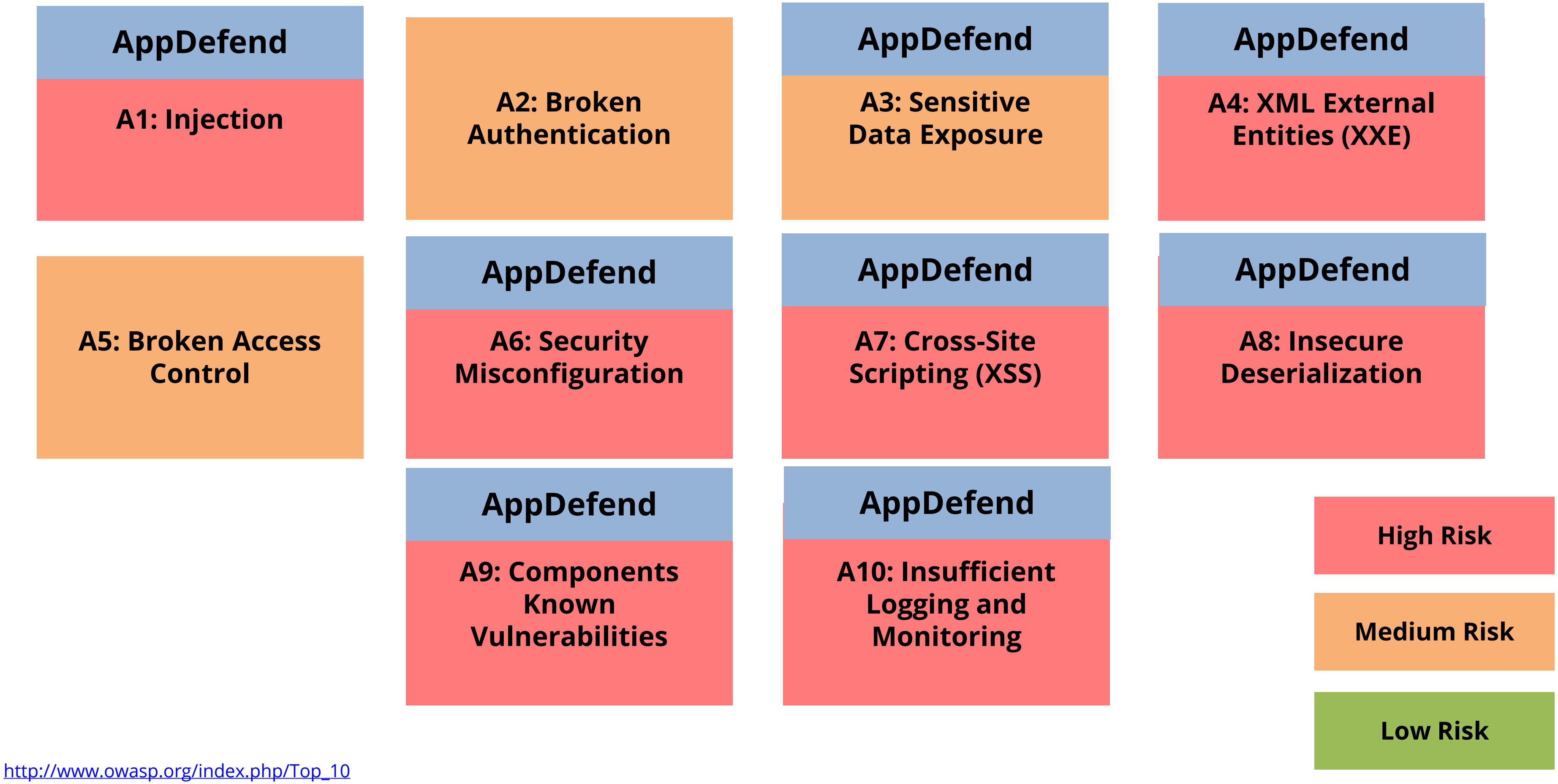
AppDefend Virtual Patching

Eliminate risk and exploitation of the security bug by blocking access to the vulnerable code

- Integrigy analyzes the Oracle Critical Patch Update (CPU)
- Delivers pre-defined rules for CPU web bugs
- Rules may be at the page or field level to block known vulnerabilities

OWASP Top 10 – AppDefend

AppDefend is the layer of defense for Oracle EBS against OWASP Top 10 security vulnerabilities.



AppDefend

A1: Injection

A2: Broken Authentication

AppDefend

A3: Sensitive Data Exposure

AppDefend

A4: XML External Entities (XXE)

A5: Broken Access Control

AppDefend

A6: Security Misconfiguration

AppDefend

A7: Cross-Site Scripting (XSS)

AppDefend

A8: Insecure Deserialization

AppDefend

A9: Components Known Vulnerabilities

AppDefend

A10: Insufficient Logging and Monitoring

High Risk

Medium Risk

Low Risk

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

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

11.2.0.4 CPU Risk Mapping – Missing One Year of CPUs

Type of User	Number of Security Bugs	Notes
Unauthenticated user No database account	3	Denial of service
Low privileged user Create session system privilege only	14	▪ Averages one per CPU ▪ Requires only PUBLIC privileges
Moderate privileged user Create table, procedure, index, etc.	10	▪ Usually requires CREATE PROCEDURE system privilege
High privileged user DBA, SYSDBA, local OS access, etc.	6	6 – SYSDBA privileges 6 – Advanced privileges 4 – Local OS access

#1 – Don’t Start Behind

- **Update to 19c if possible**
  - Supported with 12.1.3
  - Limited issues and limitations with Oracle EBS

- **ALWAYS install latest CPU with database and Oracle EBS installation or upgrades**
  - Database/EBS Install + latest PSU/SPU
  - Database/EBS Upgrade + latest PSU/SPU

- **PSU = For production, use PSU from last test DB (11.2.0.4/12c)**
- **SPU = For production, use latest SPU – low risk (11.2.0.4 only)**

Solutions by Risk for No Database CPUs

Type of User	Solutions if CPUs not applied
Unauthenticated user No database account	#2 – Limit direct access to the database #3 – Check for default passwords #4 – Use only named accounts #5 – No generic read-only accounts #6 – Change APPLSYSPUB password
Low privileged user Create session system privilege only, PUBLIC	
Moderate privileged user Create table, procedure, index, etc.	#7 – Limit privileges in production
High privileged user DBA, SYSDBA, local OS access, etc.	#8 – External database auditing solution #9 – Limit OS access for prod to DBAs #10 – Use Oracle Database Vault

#2 – Limit Database Access

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

#3 – How to Check Database Passwords

- **Use Oracle's DBA_USERS_WITH_DEFPWD**
  - Limited set of accounts
  - Single password for each account
- **Command line tools (orabf, etc.)**
  - Difficult to run – command line only
- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords

#6 – APPLSYSPUB with default password

- **Oracle EBS installs default database account APPLSYSPUB with the default password of PUB**

- **APPLSYSPUB has only limited privileges –**
  - System privileges = CREATE SESSION
  - Object privileges = Limited set of SELECT, INSERT, UPDATE, EXECUTE
  - Periodically verify no other privileges have been granted – Oracle EBS Secure Configuration Console will check APPLSYSPUB privileges

- **Oracle sees no need to change the password**

- **Able to exploit vulnerabilities in PUBLIC packages**

#7 – Limit Privileges in Production

- **The following privileges are most often referenced in CPU advisories –**

- **CREATE PROCEDURE**
  - Procedure or function is called with invoker rights thus executing as a privileged account when there is a security bug in a standard DBMS package
  - RESOURCE role is seldom required anymore

- **CREATE ANY INDEX**
  - Create a function based index
  - User queries a table with index and executes malicious code

Integrigy 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**

linkedin – **linkedin.com/company/integrigy**

twitter – **twitter.com/integrigy**