

January 15, 2007

# Security Analysis

---

## Oracle Critical Patch Update - January 2008 Oracle E-Business Suite 11i Impact

### OVERVIEW

Oracle Corporation released the thirteenth Critical Patch Update (CPU) on January 15, 2008. The CPU is a collection of security related patches for the Oracle Database, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and PeopleSoft. There are 27 vulnerabilities addressed in the CPU ranging from SQL injection to information disclosure to denial of service (DoS) issues. 17 of the 27 vulnerabilities directly affect the Oracle E-Business Suite 11i. A number of the vulnerabilities are high risk and should be addressed quickly.

This analysis provides additional information on the vulnerabilities and patches released in the CPU as they relate to the Oracle E-Business Suite 11i. The objective of this analysis is to assist IT managers and database administrators in assessing the impact on their Oracle E-Business Suite implementations and the risks associated with the vulnerabilities, especially since the CPU addresses a large number of vulnerabilities and impacts all layers of the Oracle E-Business Suite technology stack.

### CRITICAL PATCH UPDATE OVERVIEW

---

Most of the vulnerabilities fixed in the CPU are similar in nature to previous security bugs found in the Oracle Database, Oracle Application Server, and Oracle Applications – buffer overflows in standard database functions and packages, permission issues on powerful database functions, and SQL injection and parameter tampering issues in standard database functions and packages and in application web pages.

Even though the CPU does fix 27 security vulnerabilities in Oracle products, there is a large queue of unpatched security bugs (Integrigy estimates there are at least 100 open security bugs found by independent security researchers). Customers should not rely solely on these patches to provide for a secure environment. In addition to promptly applying security patches, the operating system, database, application servers, and application should be “hardened” using Integrigy’s recommendations published by Oracle in the whitepaper “Best Practices for Securing Oracle E-Business Suite” (Metalink Note 189367.1). “Defense in depth” should be employed to protect the database and application servers. Direct connections to the database using SQL\*Net should be limited to the data center and an intrusion detection or prevention solution should be deployed to detect and/or block potential attacks.

### ORACLE E-BUSINESS SUITE R12 CUMULATIVE

---

A major change to the CPU patching process for R12 is that the E-Business Suite patches are cumulative in R12 and are consolidated into a single patch. This will make patching significantly easier. Also, the January 2008 CPU patch is included in 12.0.4 (RUP4), which was released on the same day.

## ASSESSMENT OF VULNERABILITIES

For the Oracle E-Business Suite 11i, 17 of the 27 vulnerabilities are relevant and five are remotely exploitable without authentication. This analysis will only review the vulnerabilities applicable to Oracle E-Business Suite 11i and does not include information for R12.

### ORACLE DATABASE VULNERABILITIES

---

Vulnerabilities: DB01 – DB08

As with the vast majority of previous Oracle database security vulnerabilities, all of these vulnerabilities require a valid database session. Several of the database vulnerabilities can be readily exploited using the APPLSYSPUB database or any database account used for ad-hoc querying or other functions. A few of these are serious vulnerabilities and effectively allow APPLSYSPUB or any database account (e.g., ad-hoc query) to gain access to all data in the database.

#### Oracle E-Business Suite 11i Specific Database Vulnerabilities by Version and Privileges

Supported Database Version <sup>1</sup>	PUBLIC (i.e., APPLSYSPUB)	Other Privileges (CREATE VIEW)	No Default Privileges <sup>2</sup>
9.2.0.8	DB04 – SDO_CATALOG DB06 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.1.0.5	DB04 – SDO_CATALOG DB06 – Oracle Spatial DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.2.0.2/ 10.2.0.3	DB04 – SDO_CATALOG DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM

<sup>1</sup> Only Oracle Applications 11i certified and CPU supported versions are included.

<sup>2</sup> These packages are not granted any privileges by default, however, some of these packages are called by packages with PUBLIC privileges and could be exploited through these packages. Not Oracle nor any security researchers perform dependency checks to determine if the vulnerability could potentially be exploited through another package.

## **ORACLE APPLICATION SERVER VULNERABILITIES**

---

None of the Oracle Application Server vulnerabilities affect the Oracle E-Business Suite 11i. There have been no new Oracle Application Server 1.0.2.2 or Oracle Developer 6i vulnerabilities since the January 2007 CPU.

Application Server patches may be required if Oracle Application Server 10g is being used for Identity Management, SSO, or Portal.

### ***JINITIATOR VULNERABILITIES***

Two vulnerabilities impact Jinitiator 1.1.8.x and 1.3.1.x., which were previously published in September 2007 and more information is available [here](#). All Jinitiator installs need to be upgraded and all old 1.1.8.x versions must be removed from the client PC.

## **ORACLE E-BUSINESS SUITE VULNERABILITIES**

---

Vulnerabilities: APPS02, APPS03, APPS05, APPS06

### ***APPS02 – APPLICATION OBJECT LIBRARY (AOL/FND)***

A cross site scripting (XSS) issues with multiple parameters in the AppChangePassword.jsp web page.

### ***APPS03 – ORACLE APPLICATIONS FRAMEWORK***

A very minor information disclosure in the OAIInfo.jsp web page, which is stubbed in the patch.

### ***APPS05 – CRM TECHNICAL FOUNDATION***

A cross site scripting (XSS) issues in the jtflogin.jsp web page.

### ***APPS06 – APPLICATION OBJECT LIBRARY***

Implements function security for the Oracle Applications Help Utility.

## PATCH ANALYSIS

For the Oracle E-Business Suite 11i, install the patches as specified in [Oracle Metalink Note ID Note 467742.1](#) "Oracle E-Business Suite Critical Patch Update Note January 2008" and you should also review the pre-installation notes for the Oracle Database and Oracle Application Server prior to installing those patches.

### TECHNOLOGY STACK UPGRADES

---

With the release of each CPU, Oracle has required some upgrades to the technology stack by supporting only recent patchsets for the Database, Application Server, Developer 6i, JInitiator, and Applications Object Library (AOL). These required technology stack upgrades have delayed many organizations in applying the CPU patches due to the added complexity and time required to apply the security patches as well as the technology stack upgrades.

Beginning with the July 2007 CPU, the ATG\_PF RUP n-1 or ATG\_PF RUP n is required as a minimum baseline for all releases. This is for all releases including 11.5.9, which previously only required the "Rebaseline" (Metalink Note ID [363827.1](#)).

**For the January 2008 CPU, RUP4, RUP5, or RUP6 is required.**

Oracle is following strict compliance with the ATG\_PF RUP policy, therefore, Integrigy anticipates the January 2008 CPU will only support RUP 5 and RUP6.

11i.ATG\_PF.H RUP4 = 4676589 Metalink Note ID [365228.1](#) (August 2006)  
11i.ATG\_PF.H RUP5 = 5473858 Metalink Note ID [375682.1](#) (April 2007)  
11i.ATG\_PF.H RUP6 = 5903765 Metalink Note ID [444524.1](#) (October 2007)

#### ***1. ALL PREVIOUS CPUS APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES***

If you have already applied the patches from the October 2008 CPU and prior CPUs, only upgrading Jinitiator may be required.

**2. PREVIOUS CPUs NOT APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES**

The following table shows the supported patchsets (black) and unsupported patchsets (red italics) for the January 2008 CPU –

Release	Database	App Server (Apache)	Developer	JInitiator (Windows 2000/XP)	FND.x	ATG_PF
<b>11.5.1 – 11.5.8</b>	<i>Desupported</i>					
<b>11.5.9</b>	<i>9.2.0.2</i> <i>9.2.0.3*</i> <i>9.2.0.4 – 7</i> 9.2.0.8 <i>10.1.0.4</i> 10.1.0.5 10.2.0.2 – 3	<b>1.0.2.1.x*</b> <b>(1.3.12)</b> 1.0.2.2.2 (1.3.19)	<i>6.0.8.21 (P12)*</i> <i>6.0.8.x (P9 – P17)</i> 6.0.8.27 (P18)	<b>1.1.8.16*</b> <b>1.1.8.19 – 25</b> 1.1.8.27 <b>1.3.1.9 – 25</b> 1.3.1.26 – 29	<b>FND.G*</b> FND.H	11i.ATG_PF.H and (11i.ATG_PF.H RUP4 or 11i.ATG_PF.H RUP5 or 11i.ATG_PF.H RUP6)
<b>11.5.10</b>	<i>9.2.0.4</i> <i>9.2.0.5*</i> <i>9.2.0.6 – 7</i> 9.2.0.8 <i>10.1.0.4</i> 10.1.0.5 10.2.0.2 – 3	<b>1.0.2.1.x*</b> <b>(1.3.12)</b> 1.0.2.2.2 (1.3.19)	<i>6.0.8.24 (P15)*</i> <i>6.0.8.x (P16-P17)</i> 6.0.8.27 (P18)	<b>1.1.8.19 – 24</b> 1.1.8.27 <b>1.3.1.18*</b> <b>1.3.1.21-25</b> 1.3.1.26-29	FND.H*	11i.ATG_PF.H RUP4 or 11i.ATG_PF.H RUP5 or 11i.ATG_PF.H RUP6
<b>11.5.10.2</b>	<i>9.2.0.4</i> <i>9.2.0.5*</i> <i>9.2.0.6 – 7</i> 9.2.0.8 <i>10.1.0.4</i> 10.1.0.5 10.2.0.2 – 3	<b>1.0.2.1.x*</b> <b>(1.3.12)</b> 1.0.2.2.2 (1.3.19)	<i>6.0.8.24 (P15)*</i> <i>6.0.8.25 (P16-P17)</i> 6.0.8.27 (P18)	<b>1.1.8.19 – 24</b> 1.1.8.27 <b>1.3.1.18*</b> <b>1.3.1.21-25</b> 1.3.1.26-29	FND.H*	11i.ATG_PF.H RUP4 or 11i.ATG_PF.H RUP5 or 11i.ATG_PF.H RUP6

**Desupported**

**Certified, No CPU Support**

Certified, CPU Support

\* Fresh Install Version

Note: All versions are based Sun Solaris SPARC and may differ slightly based on operating system and other factors. Please use the Certify tool in Oracle Metalink and the CPU installation notes for determining the exact supported versions for your platform.

## ORACLE DATABASE PATCHES

---

The database portion of the patch fixes 6 exploitable security bugs in many components of the database and is relatively straight-forward as compared to the other CPU patches.

Oracle Database security patches are cumulative, therefore, the patches for the previous twelve CPUs (January 2005 through October 2007) and Oracle Security Alert #68 are included. Patches for all previous Oracle security alerts are also included in the database patch.

### TESTING

An abbreviated testing cycle should be performed similar to testing for a minor database updated (e.g., 9.2.0.7 to 9.2.0.8). We cannot provide specific recommendations as to where to focus testing efforts since the database patch touches all aspects of the database. For Microsoft Windows, the database patch is not a security specific patch and includes many non-security related fixes.

## ORACLE APPLICATION SERVER PATCHES

---

No patches are required for the Oracle Application Server. If Application Server patches have not been applied from previous CPUs, see the January 2007 CPU installation notes.

### TESTING

None

## ORACLE DEVELOPER 6I PATCHES

---

No patches are required for Developer 6i. If Developer 6i patches have not been applied from previous CPUs, see the January 2007 CPU installation notes.

### TESTING

None

## ORACLE JINITIATOR PATCHES

---

Oracle Jinitiator must be upgraded as follows –

Jinitiator Version	Minimum Required	Recommended Version
<b>1.1.8</b>	1.1.8.27	1.1.8.27
<b>1.3.1</b>	1.3.1.26	1.3.1.29

The recommended upgrade is to migrate from Oracle Jinitiator to the Sun Java Plug-in (see Metalink Note ID 290807.1 for more information). The Sun Java Plug-in provides an industry standard Java client environment rather than the custom Oracle Jinitiator. The Sun Java Plug-in is used natively with R12 and many other applications.

**TESTING**

Due to the integration with Oracle Forms and Jinitiator, all key and complex forms should be thoroughly tested. Testing should be similar to a Developer 6i patchset. More rigorous testing should be performed if migrating from Oracle Jinitiator to the Sun Java Plug-in.

**ORACLE E-BUSINESS SUITE PATCHES**

---

All implementations will be required to apply around 4 E-Business Suite patches. Oracle Applications 11i CPU security patches are NOT cumulative, therefore, all previous CPU patches need to be applied. Some security patches must be reapplied after version upgrades (e.g., 11.5.8 → 11.5.10.2).

The following table outlines the required patches with our assessment of importance (criticality of the security fix) and complexity (how big is the patch and probability that it will break something) along with notes about the patch. Our assessment of importance and complexity are only intended as general guidance and you will need to make a determination for your environment.

Patch	Importance	Patch Complexity	Notes
6643087	Low	Low	<ul style="list-style-type: none"> <li>▪ Oracle Applications Framework</li> <li>▪ Information disclosure in OAIInfo.jsp</li> <li>▪ No testing required</li> <li>▪ Mandatory for all implementations</li> <li>▪ Blocked by the URL Firewall for external access</li> </ul>
6142917	Medium	Low	<ul style="list-style-type: none"> <li>▪ Oracle Application Library</li> <li>▪ Implements function security for the Oracle Applications Help Utility</li> <li>▪ No testing required unless custom help pages are being loaded and then only test the actual loading</li> <li>▪ Mandatory for all implementations</li> <li>▪ Blocked by the URL Firewall for external access</li> </ul>
6640163	Medium	Low	<ul style="list-style-type: none"> <li>▪ CRM Technology Foundation (JTF)</li> <li>▪ Cross Site Scripting in the jtfflogin.jsp page</li> <li>▪ No testing required</li> <li>▪ Mandatory for all implementations</li> <li>▪ Blocked by the URL Firewall for external access</li> </ul>
6530949 or 6701339	High	Low	<ul style="list-style-type: none"> <li>▪ Application Object Library</li> <li>▪ Cross Site Scripting in the AppsChangePassword.jsp page</li> <li>▪ Test basic functionality of the reset password page</li> <li>▪ Mandatory for all implementations</li> <li>▪ Externally accessible and should be patched as soon as possible</li> </ul>

## PATCHING STRATEGY

With the number of patches required and testing effort, the patches need to be prioritized. A number of factors will affect the order and timing of the patches –

- Are the Oracle Applications application servers directly connected to the Internet?
- Does the Oracle Applications database contain sensitive data (employee information, credit card numbers, etc.)?
- Is the internal network secure?
- Can anyone directly connect to the database and execute SQL statements?
- Is there a large technical or Oracle skilled user population?

Every organization and Oracle Applications environment is unique and will have individual requirements, testing procedures, and criteria for applying security patches. The following guidelines are meant to be a reference and guide to assist you in determining how you will apply the patches.

Many of the security vulnerabilities fixed in the CPU are risk high and need to be resolved quickly. All organizations should apply all the patches recommended by Oracle as soon as possible. However, based on operational realities and patching constraints of most Oracle Applications environments, some organizations may be willing to accept the risk of not immediately patching all these security vulnerabilities.

Our recommended patching strategy differs from Oracle's recommendation of applying the database server patches, then application server patches, and finally the Oracle Applications patches. We believe our strategy will provide faster resolution of the most critical security risks, although it will leave a few high risk issues unpatched for a period of time.

### HIGH RISK AND SECURE ENVIRONMENT STRATEGY

---

This strategy assumes all patches from previous CPUs and security alerts have already been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.9 to 11.5.10 CU2) and the exact patches will depend on your version of Oracle Applications.

#### ***As Soon As Possible***

1. Apply the Oracle Database security patch as soon as possible. See Table 5 of [Oracle Metalink Note ID Note 467742.1](#) for the exact patch for your version of the Oracle Database.
2. Upgrade Jinitiator to a CPU supported version, which may require doing one of the following –
  - a. Upgrading to a new point release (e.g., 1.1.8.x to 1.1.8.27 or 1.3.1.x to 1.3.1.29)
  - b. Upgrading from 1.1.8.x to 1.3.1.29
  - c. Migrating from 1.1.8.x or 1.3.1.x to the Sun Java Plug-in
3. After upgrading Jinitiator, all previous Jinitiator versions must be either removed or have the kill bit set. See Integrigy's whitepaper on the [Jinitiator vulnerability](#) for more information.

***NEXT SCHEDULED DOWNTIME***

4. Apply the Oracle E-Business Suite patches identified in the above table as priority High or Medium. These are the most critical E-Business Suite patches.

***NEXT SCHEDULE DOWNTIME OR UPGRADE CYCLE***

5. Apply the remaining Oracle E-Business Suite patches.

**NON-HIGH RISK ENVIRONMENT STRATEGY**

---

This strategy assumes some patches from previous CPUs have not been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.9 to 11.5.10 CU2) and the exact patches will be dependent on your version of Oracle Applications. There may be other dependencies and requirements (such as upgrading to 11i.ATG\_PF.H RUP6) for your version of Oracle Applications. Due to the complexity and number of versions, it is not feasible to provide detailed guidance for every version in this analysis.

***NEXT SCHEDULED PATCH DOWNTIME***

1. Apply the Oracle Database security patch. See Table 5 of [Oracle Metalink Note ID Note 467742.1](#) for the exact patch for your version of the Oracle Database. This patch is critical and also cumulative, therefore, will correct a large number of critical security vulnerabilities. All 9iR2 instances must be upgrade to 9.2.0.8 prior to applying the security patch.
2. Upgrade Jinitiator to a CPU supported version, which may require doing one of the following –
  - a. Upgrading to a new point release (e.g., 1.1.8.x to 1.1.8.27 or 1.3.1.x to 1.3.1.29)
  - b. Upgrading from 1.1.8.x to 1.3.1.29
  - c. Migrating from 1.1.8.x or 1.3.1.x to the Sun Java Plug-in
3. After upgrading Jinitiator, all previous Jinitiator versions must be either removed or have the kill bit set. See Integrigy's whitepaper on the [Jinitiator vulnerability](#) for more information.
4. Review the required technology stack upgrades, which may include 11i.ATG\_PF.H RUP4, RUP5, or RUP6. If a RUP patch is required, RUP6 is the recommend RUP patch. Apply the necessary upgrades, including AD.I.2. 11i.ATG\_PF.H RUP6 includes many previous CPU security patches (see Metalink Note ID [365228.1](#)).
5. Apply missing critical or important Oracle E-Business Suite security patches from previous CPUs.
6. Apply the Oracle E-Business Suite patches identified in the above table as priority High. These are the most critical E-Business Suite patches.

***NEXT SCHEDULE EXTENDED DOWNTIME OR UPGRADE CYCLE***

7. Apply the Oracle Applications Server patches from January 2007 CPU if not already applied. These patches are cumulative.
8. Apply Oracle Developer 6i Patchset 18 and related patches from January 2007 CPU if not already applied. These patches are cumulative.

9. Apply any remaining Oracle E-Business Suite patches from this and previous CPUs.

## REFERENCES

### *CRITICAL PATCH UPDATE*

- Oracle Critical Patch Update January 2008 Advisory, 15 January 2008, <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

### *ORACLE DATABASE*

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 15 January 2008, [Oracle Metalink Note ID 466757.1](#)
- Oracle 9iR2 Extended Support, <http://www.oracle.com/features/hp/database-9i-support.html>

### *ORACLE APPLICATION SERVER*

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 15 January 2008, [Oracle Metalink Note ID 466757.1](#)

### *ORACLE E-BUSINESS SUITE*

- Oracle Critical Patch Update January 2008 Pre-Installation Note for Oracle E-Business Suite, 15 January 2008, [Oracle Metalink Note ID Note 467742.1](#)
- Prior E-Business Suite Security Alerts, 17 April 2007, [Oracle Metalink Note ID 315713.1](#)
- E-Business Suite (Oracle Applications) 11.5.1 through 11.5.6 Desupport Notice, 12 June 2007, [Oracle Metalink Note ID 329689.1](#)
- Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10, 11 October 2006, [Oracle Metalink Note ID 363827.1](#)
- Integrigy, Oracle Jinitiator 1.1.8 Vulnerability, 11 September 2007, <http://www.integrigy.com/oracle-security-blog/oracle-jinitiator-vulnerability>

## HISTORY

January 15, 2008 – Initial Version

## ABOUT INTEGRIGY

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

AppSentry and AppDefend have been updated to detect and/or block the vulnerabilities addressed in the Oracle Critical Patch Update – January 2008.

Integrigy Corporation  
P.O. Box 81545  
Chicago, Illinois 60602 USA  
888/542-4802  
[www.integrigy.com](http://www.integrigy.com)

Copyright © 2008 Integrigy Corporation.

Authors: Stephen Kost and Jack Kanter

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to [alerts@integrigy.com](mailto:alerts@integrigy.com).

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernable. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.