

January 17, 2007

# Security Analysis

---

Oracle Critical Patch Update – January 2007  
Oracle E-Business Suite Impact

## [ OVERVIEW ]

Oracle Corporation released the ninth Critical Patch Update (CPU) on January 16, 2007. 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 Applications. There are 51 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. 21 of the 51 vulnerabilities directly affect the Oracle E-Business Suite 11i. Many 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 (Oracle Applications 11i). The objective of this analysis is to assist IT managers and database administrators in assessing the impact on their Oracle Applications 11i 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 Applications 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 over 50 security vulnerabilities, there is a large queue of unpatched security bugs. There are more than 100 open security bugs found by independent security researchers in all layers of the technology stack and many of these bugs are deemed high risk. Also, there are reports that some of the security bugs identified as fixed by Oracle in previous CPUs, are still exploitable due to errors in the patches or because Oracle implemented inadequate fixes. The most disconcerting issue is that the same packages keep appearing in the CPUs - `sys.dbms_capture_adm_internal` (January 2006) and `sys.dbms_cdc_subscribe` (October 2005).

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.

## ASSESSMENT OF VULNERABILITIES

For the Oracle E-Business Suite, 21 of the 51 vulnerabilities are relevant and seven are remotely exploitable without authentication (all of which are Oracle Application Server vulnerabilities). This analysis will only review the vulnerabilities applicable to Oracle Applications 11i.

### ORACLE DATABASE VULNERABILITIES (DB01 – DB16)

Many of the database vulnerabilities (DB01-DB09) can easily be exploited using a direct SQL\*Net connection to the database or indirect connection (e.g., reporting tools) that allows a user to execute arbitrary SQL statements. This is especially a problem with Oracle Applications, unless specifically blocked, given that anyone can access the database and logon using the APPLSYSPUB account; the APPLSYSPUB database account has a well known password and can not be disabled. A few of these vulnerabilities can be exploited using the APPLSYSPUB database account, since APPLSYSPUB has access to all of the vulnerable database packages by default.

*Table 1 – Summary of Database Vulnerabilities*

ID	Component/Object	Type of Vulnerability
DB01	sys.dbms_aq	SQL Injection ( <a href="#">ref</a> )
DB02	sys.dbms_cdc_subscribe	Buffer Overflow
DB03	sys.dbms_drs	Buffer Overflow
DB04	sys.dbms_logmnr	Buffer Overflow
DB05	mdsys.md	Buffer Overflow
DB06	XMLDB	Cross-site Scripting ( <a href="#">ref</a> )
DB07	sys.dbms_repcat_untrusted	Buffer Overflow
DB08	sys.dbms_logrep_util	Buffer Overflow
DB09	sys.dbms_capture_adm_internal	Buffer Overflow

The following table shows for each database version the vulnerabilities that can be exploited using the APPLSYSPUB account.

*Table 2 – Database Vulnerabilities by Version and Privileges*

Supported Database Version <sup>1</sup>	Remotely Exploitable and Requires No Authentication	PUBLIC (i.e., APPLSYSPUB)	Privileged Role (AQ_USER_ROLE, EXECUTE_CATALOG_ROLE, OEM_MONITOR, etc.)
9.2.0.7	DB06 <sup>2</sup> - XDB	DB01 - dbms_aq DB02 - dbms_cdc_subscribe DB05 - md	DB03 - dbms_drs DB04 - dbms_logmnr
9.2.0.8	DB06 <sup>2</sup> - XDB	DB02 - dbms_cdc_subscribe	
10.1.0.4	DB06 <sup>2</sup> - XDB	DB01 - dbms_aq DB02 - dbms_cdc_subscribe DB05 - md	DB03 - dbms_drs
10.1.0.5	DB06 <sup>2</sup> - XDB	DB01 - dbms_aq DB02 - dbms_cdc_subscribe	
10.2.0.2	DB06 <sup>2</sup> - XDB	DB02 - dbms_cdc_subscribe	

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

<sup>2</sup> XML DB (XDB) is an optional database component and may not be installed in your database.

<sup>3</sup> DB07, DB08, and DB09 are not granted by default to any database accounts or roles.

In addition, most of these vulnerabilities can be exploited via SQL injection vulnerabilities in Oracle Applications. Attacks on the database server can be made using a web browser, even though the attacker does not have direct access to the database server. This possibility will have the greatest impact on those implementations where Oracle Applications web servers are directly connected to the Internet.

The remaining vulnerabilities DB10-DB16 require local operating system privileges in order to execute the vulnerable binaries (e.g., tnslnr and ctxload). In all Oracle Applications 11i environments, it is highly unlikely an attacker would have sufficient privileges in order to execute these binaries and exploit the vulnerability.

## ORACLE APPLICATION SERVER VULNERABILITIES

---

Vulnerabilities: OHS01, OHS02, OHS05, OHS06, OHS07, REP01

### *OHS01 – OPENSLL BUFFER OVERFLOW*

OHS01 ([CVE-2006-3738](#)) is a vulnerability in the OpenSSL (mod\_ssl) component of the Oracle HTTP Server and is only exploitable if SSL is configured. If an external SSL accelerator (not the native Oracle HTTP Server mod\_ssl) is being used, then the Oracle HTTP Server is not vulnerable to this issue. This vulnerability is a buffer overflow bug, which may allow an attacker to execute operating system commands as the oracle or applmgr Unix accounts.

### *OHS02, OHS05, OHS06 – OPENSLL VULNERABILITIES*

OHS02 ([CVE-2006-4339](#)), OSH05 ([CVE-2006-2940](#)), and OHS06 ([CVE-2006-4343](#)) are vulnerabilities in the OpenSSL (mod\_ssl) component of the Oracle HTTP Server. If an external SSL accelerator (not the native Oracle HTTP Server mod\_ssl) is being used, then the Oracle HTTP Server is not vulnerable to this issue. OSH05 and OSH06 are denial of service vulnerabilities. OSH02 is a bug that may cause OpenSSL to incorrectly verify a certificate, which would only be exploitable in implementations that rely on certificates for authentication or trust relationships. In an Oracle Applications 11i environment, this may be an issue with external partner interfaces (such as using XML Gateway as described in Metalink Note ID [152775.1](#)).

### *REP01 – REPORT SERVER VULNERABILITY*

An unspecified vulnerability exists in the Oracle Reports Server that can be remotely exploited without authentication. **The Oracle Reports Server should be disabled whenever possible and should never be directly accessible from the Internet.** See the "Disabling the Oracle Reports Server" section of this document for more information on disabling the Reports Server.

## ORACLE E-BUSINESS SUITE VULNERABILITIES

---

Vulnerabilities: APPS01 – APPS06, OWF01

There are only two security vulnerabilities fixed by the Oracle Applications January 2007 CPU patches. Oracle is continuing a trend of including fixes for security weaknesses in the Oracle E-Business Suite in the quarterly CPUs. Previous CPUs have corrected numerous information disclosure issues. Most of the patches included in this CPU can be classified more as fixing security weaknesses rather than critical security vulnerabilities – such a weakness would be storing passwords as plain text.

***APPS02 – MULTIPLE WEB APPLICATIONS DESKTOP INTEGRATOR ISSUES***

There are multiple security vulnerabilities in WEB ADI including potential authentication, cross-site scripting (XSS), and SQL injection vulnerabilities.

***APPS03 AND APPS05 – PLAIN-TEXT PASSWORDS***

These issues are instances of Oracle Applications storing passwords as plain text in system profile option values. All these passwords are ancillary passwords used by individual modules.

***OWF01 – CROSS SITE SCRIPTING***

OWF01 are multiple cross-site scripting (XSS) issues in Oracle Workflow PL/SQL packages.

***APPS04 – ACCOUNTS PAYABLE SENSITIVE INFORMATION DISPLAYED***

APPS04 is an issue in Accounts Payable where the taxpayer ID field is displayed in forms and reports when an employee is setup as a vendor.

***APPS01 – APPS PASSWORD IN LOG FILE***

APPS01 is an issue where the APPS password is written to a standard Oracle Applications log file.

## [ PATCH ANALYSIS ]

For the Oracle E-Business Suite, install the patches as specified in Metalink ID Note [402670.1](#) "Oracle E-Business Suite Critical Patch Update Note January 2007" 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 2006 CPU, Oracle has mandated the minimum 11i ATG\_PF baseline for all security patches as outlined in Metalink Note [363827.1](#) "Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10". This may mean

significant applications technology stack upgrades, especially for environments that have not been recently upgraded. Also, the baseline is dynamic and is continuously updated by Oracle, although, the updates to date have not been significant.

Beginning with the October 2006 CPU, Oracle requires 11.5.10, 11.5.10.1 (CU1), and 11.5.10.2 (CU2) have the Oracle Applications Technology 11i.ATG\_PF.H RUP3 (4334965) or 11i.ATG\_PF.H RUP4 (4676589) applied [Oracle recommends RUP4]. For the July 2007 CPU and onwards, ATG\_PF RUP n-1 or ATG\_PF RUP n will be required as a minimum baseline for all releases.

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

If you have already applied the patches from the October 2006 CPU and prior CPUs, the only significant changes are –

- Oracle Database 9.2.0.6 CPU patch is no longer certified for the Oracle E-Business Suite
- Oracle Developer 6.0.8.26 (Patchset 17) is no longer certified, therefore, the latest Patchset (18) must be installed

**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 2007 CPU –

Release	Database	App Server (Apache)	Developer	JInitiator (WinXP)	FND.x	ATG_PF
<b>11.5.1-6</b>	<i>Desupported</i>					
11.5.7	<i>8.1.7.3</i> <i>8.1.7.4*</i> <i>9.2.0.2 – 6</i> 9.2.0.7 9.2.0.8	<i>1.0.2.1.x*</i> <i>(1.3.12)</i> 1.0.2.2.2 (1.3.19)	<i>6.0.8.18 (P9)*</i> <i>6.0.8.x (P10 – P17)</i> 6.0.8.27 (P18)	<i>1.1.8.16*</i> <i>1.1.8.19 – 24</i> 1.1.8.25 <i>1.3.1.9 – 18</i> 1.3.1.21-26	<i>FND.E*</i> <i>FND.F</i> FND.G FND.H	Rebaselined per Metalink Note ID 363827.1
11.5.8	<i>8.1.7.4</i> <i>9.2.0.2</i> <i>9.2.0.3*</i> <i>9.2.0.4 – 6</i> 9.2.0.7 9.2.0.8	<i>1.0.2.1.x*</i> <i>(1.3.12)</i> 1.0.2.2.2 (1.3.19)	<i>6.0.8.18 (P9)*</i> <i>6.0.8.x (P10 – P17)</i> 6.0.8.27 (P18)	<i>1.1.8.16*</i> <i>1.1.8.19 – 24</i> 1.1.8.25 <i>1.3.1.9 – 18</i> 1.3.1.21-26	<i>FND.F*</i> FND.G – H	Rebaselined per Metalink Note ID 363827.1
11.5.9	<i>9.2.0.2</i> <i>9.2.0.3*</i> <i>9.2.0.4 – 6</i> 9.2.0.7 9.2.0.8 10.1.0.4 10.1.0.5 10.2.0.2	<i>1.0.2.1.x*</i> <i>(1.3.12)</i> 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)	<i>1.1.8.16*</i> <i>1.1.8.19 – 24</i> 1.1.8.25 <i>1.3.1.9 – 18</i> 1.3.1.21-26	FND.G* FND.H	Rebaselined per Metalink Note ID 363827.1
11.5.10	<i>9.2.0.4</i> <i>9.2.0.5*</i> <i>9.2.0.6</i> 9.2.0.7 10.1.0.4 10.1.0.5 10.2.0.2	<i>1.0.2.1.x*</i> <i>(1.3.12)</i> 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)	<i>1.1.8.19 – 24</i> 1.1.8.25 <i>1.3.1.18*</i> 1.3.1.21-26	FND.H*	11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4
11.5.10.2	<i>9.2.0.4</i> <i>9.2.0.5*</i> <i>9.2.0.6</i> 9.2.0.7 9.2.0.8 10.1.0.4 10.1.0.5 10.2.0.2	<i>1.0.2.1.x*</i> <i>(1.3.12)</i> 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)	<i>1.1.8.19 – 24</i> 1.1.8.25 <i>1.3.1.18*</i> 1.3.1.21-26	FND.H*	11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4

**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 nine remotely 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 eight CPUs (January 2005 through October 2006) and Oracle Security Alert #68 are included. Patches for all previous Oracle security alerts are also included in the database patch. See Metalink Note [237007.1](#) "FAQ for Security Alerts and Critical Patch Updates" question #13 for more details on the exact patches included in each update.

The scope and size of the database patches are increasing with each CPU and it appears that non-security related bugs are being fixed in the patches. Reviewing the patches for 9.2.0.6 on Solaris shows –

**Table 4 – CPU Database Patch Size and Bug Count**

Critical Patch Update	Size of Patch Download File	Bugs Identified in Readme.html*
April 2005	2.6 MB	1
July 2005	3.8 MB	8
October 2005	7.6 MB	38
January 2006	10.8 MB	86
April 2006	13.0 MB	124
July 2006	14.1 MB	160

\* The number of bugs identified is not accurate because many of the bug numbers listed in the Readme file are actually "merge" bugs (groups of bugs).

As an example of a non-security related bug, the January 2006 9.2.0.6 patch fixes the bug titled "3817792:ORA-600 [6100] WHILE COALESCING AN INDEX". Either Oracle is including general fixes in the security patches or this bug fix must be included due to dependencies.

### TESTING

An abbreviated testing cycle should be performed similar to testing for a minor database updated (e.g., 9.2.0.4 to 9.2.0.6). We can not 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

---

### *1.0.2.1.x*

The patches for the Oracle Application Server require de-supported 1.0.2.1.x environments to upgrade to 1.0.2.2.x, which is significant as this upgrade requires a full installation of 1.0.2.2.x and implementation of AutoConfig as well as the installation of the latest Developer 6i PatchSet.

### *1.0.2.2.x*

The CPU requires the 1.0.2.2.x Oracle Home be upgraded to 8.1.7.4, if already not done so.

Patch 5700129 is cumulative for all previous CPUs and includes a number of updates to key Apache and 8.1.7.4 binaries. There are no updates to mod\_plsql in the July 2006, October 2006, or January 2007 CPUs.

### *TESTING*

Since these patches impact both Apache and Jinitiator, a brief walk-through and execution of critical web pages and Forms should be performed to test the patches.

No additional testing should be required for the mod\_plsql component of the patch as there are no updates in this CPU since April 2006.

## ORACLE DEVELOPER 6I PATCHES

---

The security patches for Developer 6i require PatchSet 18 be applied, which can be a significant undertaking. The patch is 253MB and may require an additional 8 patches depending on operating system.

There are two security patches required for Developer 6i – (1) an Oracle Forms patch 5687261 and (2) an Oracle Reports patch 5686997. These patches are cumulative, so only the patches from the most recent CPU have to be applied.

### *TESTING*

The Developer 6i patches may affect behavior of Forms, thus, critical and highly used Oracle Applications Forms should be tested.

## ORACLE JINITIATOR PATCHES

---

There are no new vulnerabilities in Oracle JInitiator for the January 2007 CPU.

## ORACLE E-BUSINESS SUITE PATCHES

Most implementations will be required to apply around 6 E-Business Suite patches. All supported versions appear to be impacted equally with a similar number of patches and patch complexity. 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). The only exception for this CPU is the Technology Stack patch 5658489.

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.

*Table 5 – Oracle E-Business Suite CPU Patch Summary*

Patch	Importance	Complexity	Notes
5658489	High	Medium	<ul style="list-style-type: none"> <li>▪ Technology Stack Templates</li> <li>▪ Patch includes October 2006 CPU patch 5447522</li> <li>▪ This patch includes updated AutoConfig templates Rollup Patch O (December 2006)</li> <li>▪ Test Forms and all custom forms applications integrated into Oracle Applications</li> <li>▪ If the October 2006 CPU patch 5447522 was applied, no testing is required</li> </ul>
3578012 5518587	High	Medium	<ul style="list-style-type: none"> <li>▪ Fixes multiple issues with Web ADI and should be applied for all implementations regardless if Web ADI is installed or configured</li> <li>▪ The patch is in essence a RUP for BNE.C or BNE.D, not just a single security fix</li> <li>▪ Test all functions within Web ADI as this patch may be significant based on the currently installed version</li> </ul>
5571208 5571211	Medium	Medium	<ul style="list-style-type: none"> <li>▪ Fixes for cross-site scripting issues in Oracle Workflow</li> <li>▪ For 11.5.7-11.5.9, these patches may require a significant pre-requisite workflow patch (OWF.G. RUP7)</li> <li>▪ Only minimal testing of workflow should be required</li> </ul>
5711485 5711481 5714480 5711474 5729389 5744932	Medium	High	<ul style="list-style-type: none"> <li>▪ Fixes display issues of employee taxpayer IDs in the Supplier Entry form and reports</li> <li>▪ Test the Supplier Entry form, all processing related to 1099, and 1099 reports such 'Tax Identification Number Letter' and '1099 Forms - Comma Delimited'</li> </ul>
3748835 5724734	Low	Low	<ul style="list-style-type: none"> <li>▪ Fixes storing of plain-text password for HR Research Institute of America (RIA) integration</li> <li>▪ This patch is probably only required if RIA integration is configured</li> <li>▪ Test any RIA integration</li> </ul>
5661618 3748840 5661619 5661617	Medium	Medium	<ul style="list-style-type: none"> <li>▪ Fixes storing of plain-text password for TCA integration with DNB</li> <li>▪ This patch is probably only required if DNB integration is configured</li> <li>▪ Test any DNB integration</li> </ul>
5396733 5698867	Low	Low	<ul style="list-style-type: none"> <li>▪ Windows Only</li> <li>▪ Fixes writing of APPS password log files</li> <li>▪ Test ability to start and stop the Concurrent Manager service</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 (11.5.7 to 11.5.10 CU2) and the exact patches will depend on your version of Oracle Applications.

#### ***AS SOON AS POSSIBLE***

1. Disable the Oracle Reports Server if it is not required and not already disabled. This may have already been done as part of the January 2006 CPU. See the next section "Disabling the Oracle Reports Server" for more information.

2. Apply the Oracle Database security patches as soon as possible. See Table 1 of Metalink Note ID [402670.1](#) for the exact patch for your version of the Oracle Database. We recommend all implementations prioritize this patch as critical.

#### ***NEXT SCHEDULED DOWNTIME***

3. Apply Oracle HTTP Server patch 5700129, which assumes the Application Server has been upgraded to 1.0.2.2.2 and its Oracle Home to 8.1.7.4. If Oracle Applications is directly connected to the Internet and is natively running SSL (not through an external SSL accelerator), you should prioritize this patch.
4. Apply the Oracle E-Business Suite patches identified in the above Table 4 as priority High or Medium. These are the most critical E-Business Suite patches.

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

5. Apply Oracle Developer 6i Patchset 18, if already not done so. Apply the Developer 8.0.6 Oracle Home, Oracle Forms, and Oracle Reports security patches. See Table 3 for details from Metalink Note ID [402670.1](#).
6. 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 (11.5.7 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 RUP4) 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 DOWNTIME***

1. Disable the Oracle Reports Server if it is not required and not already disabled. This may have already been done as part of the January 2006 CPU. See the next section "Disabling the Oracle Reports Server" for more information.
2. Apply the Oracle Database security patches as soon as possible. See Table 1 of Metalink Note ID [402670.1](#) for the exact patch for your version of the Oracle Database. We recommend all implementations prioritize this patch as critical. This patch is critical and also cumulative, therefore, will correct a large number of critical security vulnerabilities.

***NEXT SCHEDULED PATCH DOWNTIME***

3. Review the required technology stack upgrades, which may include 11i.ATG\_PF.H RUP4 for 11.5.10.x. Apply the necessary upgrades, including AD.I.x. 11i.ATG\_PF.H RUP4 includes many previous CPU security patches (see Metalink Note ID [365228.1](#)).
4. Apply 5658489 (cumulative technology stack patch) as this patch includes the latest AutoConfig templates and patches a number of number vulnerabilities. Do not apply patches 5183582 (July 2006 CPU) or 5447522 (October 2006 CPU) since 5658489 replaces these patches.
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 4 as priority High. These are the most critical E-Business Suite patches.

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

7. Apply Oracle HTTP Server patch 5700129, which assumes the Application Server has been upgraded to 1.0.2.2.2 and its Oracle Home to 8.1.7.4. If Oracle Applications is directly connected to the Internet and is natively running SSL (not through an external SSL accelerator), you should prioritize this patch.
8. Apply Oracle Developer 6i Patchset 18, if already not done so. Apply the Developer 8.0.6 Oracle Home, Oracle Forms, and Oracle Reports patches. See Table 3 for details from Metalink Note ID [402670.1](#).
9. Apply any remaining Oracle E-Business Suite patches from this and previous CPUs.

## [ DISABLING THE ORACLE REPORTS SERVER ]

There are a number of security vulnerabilities and security weaknesses in the Oracle Reports Server 6i. The Report Server is only used by a few Oracle Applications modules and can be safely disabled if these modules are not used. The following modules require the Oracle Reports Server –

ABM - Activity Based Management

BIC - Oracle Customer Intelligence

BIL - Oracle Sales Intelligence

BOM - Bill Of Materials

FII - Oracle Financials Intelligence

HRI - Human Resources Intelligence

INV - Inventory

MRP - Material Resource Planning

POA - Purchasing Intelligence

QA - Oracle Quality

WIP - Work In Progress

If the Reports Server is not required, use the AutoConfig Context Editor or the OAM web-based Context Editor to set the Applications context variable –

```
s_reptstatus = disabled
```

See Metalink Note ID [393811.1](#) for more information on determining if the Oracle Reports Server is enabled.

## [ REFERENCES ]

1. Oracle Corporation, "Oracle Critical Patch Update January 2007 Advisory", Metalink Note ID [403335.1](#), 16 January 2007
2. Oracle Corporation, "Oracle E-Business Suite Critical Patch Update Note January 2007", Metalink Note ID [402670.1](#), 16 January 2007
3. Oracle Corporation, "[Map of Public Vulnerability to Advisory/Alert](#)", 16 January 2007
4. Red Database Security, "[http://www.red-database-security.com/advisory/oracle\\_cpu\\_jan\\_2007.html](http://www.red-database-security.com/advisory/oracle_cpu_jan_2007.html)", 16 January 2007
5. Oracle Corporation, "Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10", Metalink Note ID [363827.1](#), 11 October 2006

## [ HISTORY ]

January 17, 2007 – 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 2007.

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

Copyright © 2007 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.