

October 20, 2006

Security Analysis

Oracle Critical Patch Update – October 2006
Oracle E-Business Suite Impact

[OVERVIEW]

Oracle Corporation released the eighth Critical Patch Update (CPU) on October 17, 2006. 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 more than 101 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. Most 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 100 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 this and previous CPUs, are still exploitable due to errors in the patches or because Oracle implemented inadequate fixes.

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, 42 of the 101 vulnerabilities are relevant and 7 are remotely exploitable (all of which are Oracle Application Server vulnerabilities). This analysis will only review the vulnerabilities applicable to Oracle Applications 11i.

With information released by Oracle and security researchers and since most of the vulnerabilities are similar in nature to previous vulnerabilities, we believe usable exploits can be easily developed for some of the vulnerabilities in a matter of hours.

ORACLE DATABASE VULNERABILITIES (DB01 – DB22)

Many of the database vulnerabilities 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 APPLSYS PUB account; the APPLSYS PUB database account has a well known password and can not be disabled. Almost all of these vulnerabilities can be exploited using the APPLSYS PUB database account, since APPLSYS PUB has access to all of the vulnerable database packages by default.

The following table shows for each database version the vulnerabilities that can be exploited using the APPLSYS PUB account. With the exception of DB02, anyone of these vulnerabilities can be used to select sensitive data owned by the APPS account and potentially also insert, update, or delete data. A number of the vulnerabilities are SQL injection bugs in standard Oracle database packages that allow for arbitrary SQL to be executed under the SYS account.

Table 1 – Database Vulnerabilities by Version and Privileges

Supported Database Version ¹	PUBLIC (i.e., APPLSYS PUB)	Create Session (i.e., APPLSYS PUB)	Create Session + Create Procedure ²
9.2.0.6	DB03 DB11 DB13 DB18 DB20 DB21 DB22 <u>Optional Components</u> DB01 ³ DB05 ⁴ DB06 ⁴ DB15 ³	DB09 DB14 ³ DB17	
9.2.0.7	DB03 DB11 DB13 DB20 DB21 DB22 <u>Optional Components</u> DB05 ⁴ DB06 ⁴ DB15 ³	DB09 DB14 ³ DB17	
10.1.0.4	DB03 DB10 DB11 DB12 DB13 DB20 DB21 DB22 <u>Optional Components</u> DB01 ³ DB04 ⁴ DB05 ⁴ DB06 ⁴ DB07 ⁴ DB08 ⁴ DB15 ³ DB16 ⁴	DB09 DB14 ³ DB17	
10.1.0.5	DB03 DB10 DB12 DB13 <u>Optional Components</u> DB04 ⁴ DB05 ⁴ DB06 ⁴ DB07 ⁴ DB08 ⁴ DB15 ³ DB16 ⁴	DB09 DB14 ³ DB17	
10.2.0.2	DB13	DB09 DB14 ³ DB14	DB02
¹ Only Oracle Applications 11i certified and CPU supported versions are included. ² Both CREATE SESSION and CREATE PROCEDURE privileges are required to exploit the vulnerability. ³ XML DB (XDB) is an optional database component and may not be installed in your database. ⁴ Change Data Capture (CDC) is an optional database component and may not be installed in your database.			

The most noteworthy bug fixed is DB09 (in-line views security bug), which allows an attacker with only CREATE SESSION system privilege and only select permissions on a table is able to insert, update, or delete data in the table.

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 package SYS.DBMS_CDC_IMPDP (DB04) was also fixed in the October 2005 CPU and July 2006 CPU, which again shows Oracle is not thoroughly reviewing vulnerable code for other potential vulnerabilities.

ORACLE APPLICATION SERVER VULNERABILITIES

Vulnerabilities: FORM02, OHS02, OHS05, OHS06, OHS08, REP01, REP02

REP01 AND REP02 – REPORT SERVER CROSS SITE SCRIPTING

These two vulnerabilities are cross site scripting (XSS) bugs in the Oracle Reports Server and can be exploited in a targeted attack. **The Oracle Reports Server should be disabled whenever possible and should never be directly accessible from the Internet.** See the Patch Strategy section of this document for more information on disabling the Reports Server.

OHS06 – APACHE EXPECT HEADER INJECTION

OHS06 ([CVE-2006-3918](#)) is a vulnerability in the Apache web server processing of the Expect header, which could be used in a targeted XSS attack. This is slightly more complicated to exploit than REP01 or REP02 as it requires the client to execute client-side code, such as a Flash object.

OHS05 – SSL CLIENT CERTIFICATES

OHS05 ([CVE-2005-2700](#)) is an SSL vulnerability specific to mod_ssl used by Oracle Applications 11i. If you are using are not using SSL or are using an external SSL accelerator, then Oracle HTTP Server (i.e., Apache) is not vulnerable to this issue. Only if SSL client authentication is being used and the SSLVerifyClient is configured in a specific way is this vulnerability exploitable (see Metalink Note ID [251167.1](#) and [250748.1](#) for more information on SSL client authentication). 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](#)).

OHS02 AND OHS08 – LOCAL OPERATING SYSTEM EXPLOITS

These two vulnerabilities can only effectively be exploited locally (i.e., via operating system access) in Oracle Applications 11i. OHS02 ([CVE-2005-0109](#)) is a buffer overflow in the Apache htdigest program, which is typically not used in an 11i environment. OHS08 ([CVE-2005-0109](#)) is an issue specific to Intel Hyper-Threading CPUs (including Xeon), where a local attacker is able to steal cryptographic keys and other sensitive information.

FORMS02 – FORMS SERVER DENIAL OF SERVICE

This is a denial of service (DoS) vulnerability within the Oracle Forms server.

ORACLE E-BUSINESS SUITE VULNERABILITIES (APPS02 – APPS13)

There are no critical security vulnerabilities fixed by any of the Oracle Applications October 2006 CPU patches. Oracle is continuing a trend of including fixing 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 security weaknesses rather than critical security vulnerabilities – such a weakness would be storing passwords as plain text.

APPS03, APPS05, APPS06, APPS07, APPS09, AND APPS10 – PLAIN-TEXT PASSWORDS

These fix the storing of passwords as plain text, mostly in system profile option values. All these passwords are ancillary passwords used by individual modules. APPS03 is an improvement to the security of the new FND_VAULT, used for storing passwords and credit card encryption.

APPS02 AND APPS08 – CROSS SITE SCRIPTING

APP02 and APPS08 are cross site scripting (XSS) in the login page and iStore.

APPS13 – CONFIGURATOR PERMISSION ISSUE

APPS13 is a Configurator permission issue in the Oracle Install Base module that may allow a read-only user to perform updates.

APPS04 – DENIAL OF SERVICE

APPS04 is a denial of service issue based on the CVSS scoring.

[PATCH ANALYSIS]

For the Oracle E-Business Suite, install the patches as specified in Metalink ID Note [391564.1](#) “Oracle Critical Patch Update October 2006 Pre-Installation Note for Oracle E-Business Suite” 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 July 2006 CPU and prior CPUs, the only significant changes are –

- The October 2006 CPU 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.
- Oracle Database 8.1.7.4 has been de-supported for 11.5.7 and 11.5.8 and no security patches are available.

2. PREVIOUS CPUs NOT APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES

The following table shows the supported patchsets (black) and unsupported patchsets (red italics) for the October 2006 CPU –

Table 2 – CPU Supported Technology Stack Versions

Release	Database	App Server (Apache)	Developer	JInitiator (WinXP)	FND.x	ATG_PF
<i>11.5.1</i>	<i>11.5.1 – 11.5.6 Desupported</i>					
<i>11.5.2</i>						
<i>11.5.3</i>						
<i>11.5.4</i>						
<i>11.5.5</i>						
<i>11.5.6</i>						
11.5.7	<i>8.1.7.3</i> <i>8.1.7.4*</i> <i>9.2.0.2 – 5</i> 9.2.0.6 9.2.0.7	<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 – P16)</i> 6.0.8.26 (P17)	<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 – 5</i> 9.2.0.6 9.2.0.7	<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 – P16)</i> 6.0.8.26 (P17) 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 – 5</i> 9.2.0.6 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>6.0.8.21 (P12)*</i> <i>6.0.8.x (P9 – P16)</i> 6.0.8.26 (P17) 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> 9.2.0.6 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>6.0.8.25 (P16)</i> 6.0.8.26 (P17) 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> 9.2.0.6 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>6.0.8.25 (P16)</i> 6.0.8.26 (P17) 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

ORACLE DATABASE PATCHES

The database portion of the patch fixes over 22 security related bugs in many components of the database and is relatively straight-forward as compared to the other CPU patches.

The following database patches have been delayed until the end of October –

- 9.2.0.6 on Linux, Unix, and Windows
- 10.1.0.5 on Linux, Unix, and Windows
- 10.2.0.2 on Windows

Oracle Database security patches are cumulative, therefore, the patches for the previous seven CPUs (January 2005 through July 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 3 – 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
October 2006	not yet released	?

* 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). Testing should be more rigorous than previous CPU database patches since this patch fixes many more bugs and includes non-security related fixes.

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 5483331 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 or October 2006 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 requires PatchSet 17 or 18 be applied, which can be a significant undertaking. The patches are around 220MB and may require an additional 8 patches depending on operating system.

There are three sets of security patches required for Developer 6i – (1) a patch for the 8.0.6 ORACLE_HOME to fix issues in the Oracle client software, (2) an Oracle Forms patch, and (3) an Oracle Reports patch. All of 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 October 2006 CPU.

ORACLE E-BUSINESS SUITE PATCHES

Most implementations will be required to apply around 6 E-Business Suite patches. All supported version appear to be impacted equally with 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 5447522.

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 4 – Oracle E-Business Suite CPU Patch Summary

Patch	Importance	Complexity	Notes
5447522	High	Medium	<ul style="list-style-type: none"> Technology Stack Templates Patch includes July 2006 CPU patch 5183582 Test Forms and all custom forms applications integrated into Oracle Applications
5486407 5486408	High	Low	<ul style="list-style-type: none"> This patch only affects the AppsLocalLogin.jsp file 11i.ATG_PF.H RUP4 does not need to apply this patch
5479643	Medium	Low	<ul style="list-style-type: none"> Enhancements to the FND Vault
5521537 3748842 5521476 5526897	Medium	Medium	<ul style="list-style-type: none"> Trading Community Architecture (TCA), but should be applied by all implementations
4580011 4665644	Medium	Medium	<ul style="list-style-type: none"> Install Base Configurator only
5500118	Low	Low	<ul style="list-style-type: none"> Fix plain-text passwords in profile options in various modules, but should be applied by all implementations Review the profile options changed in the fndprfh.sql SQL script to determine appropriate testing
5335967 5549676 5549711	Low	Low	<ul style="list-style-type: none"> iStore, but should be applied by all implementations
5483388 5483382 5483377	Low	Medium	<ul style="list-style-type: none"> Mobile Field Service only
5534762 5534752 5534742	Low	Low	<ul style="list-style-type: none"> E-mail Center only

[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 [391564.1](#) for the exact patch for your version of the Oracle Database. We recommend all

implementations prioritize this patch as critical, although, several database patches will not be available until the end of October.

NEXT SCHEDULED DOWNTIME

3. 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

4. Apply Oracle HTTP Server patch 5483331, 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, you should prioritize this patch and apply it during the next scheduled downtime.
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 [391564.1](#).
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 [391564.1](#) for the exact patch for your version of the Oracle Database. We recommend all implementations prioritize this patch as critical, although, several database patches will not be available until the end of October. This patch is critical and also cumulative, therefore, will correct a large number of critical security vulnerabilities.

NEXT SCHEDULED EXTENDED 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 missing critical or important Oracle E-Business Suite security patches from previous CPUs. Do not apply patch 5183582 from the July 2006 CPU – the replacement patch will be applied next.
5. 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 DOWNTIME OR UPGRADE CYCLE

6. Apply Oracle HTTP Server patch 5483331, 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, you should prioritize this patch and apply it during the next scheduled downtime.
7. 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 [391564.1](#).
8. 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 October 2006 Advisory", Metalink Note ID [391558.1](#), 17 October 2006
2. Oracle Corporation, "E-Business Suite Critical Patch Update October 2006 Note", Metalink Note ID [391564.1](#), 17 October 2006
3. Oracle Corporation, "[Map of Public Vulnerability to Advisory/Alert](#)", 19 October 2006
4. Red Database Security, "[Details Oracle Critical Patch Update October 2006 - V1.00](#)", 18 October 2006

[HISTORY]

October 20, 2006 – 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 – October 2006.

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60602 USA
888/542-4802
www.integrigy.com

Copyright © 2006 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.

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.