

April 21, 2008

Security Analysis

Oracle Critical Patch Update – April 2008 Oracle E-Business Suite 11i and R12 Impact

OVERVIEW

Oracle Corporation released the fourteenth Critical Patch Update (CPU) on April 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, PeopleSoft, and Siebel. There are 41 vulnerabilities addressed in the CPU ranging from SQL injection to information disclosure to denial of service (DoS) issues. 24 of the 41 vulnerabilities directly affect the Oracle E-Business Suite 11i and 22 of the 41 vulnerabilities directly affect the Oracle E-Business Suite R12. 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 and R12. 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 41 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.

ASSESSMENT OF VULNERABILITIES

For the Oracle E-Business Suite 11i, 24 of the 41 vulnerabilities are relevant and seven are remotely exploitable without authentication. For the Oracle E-Business Suite R12, 22 of the 41 vulnerabilities are relevant and five are remotely exploitable without authentication. This analysis will only review the vulnerabilities applicable to Oracle E-Business Suite and does not include vulnerabilities for other Oracle products.

ORACLE DATABASE VULNERABILITIES

Vulnerabilities: DB01 – DB15

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 and R12 Specific Database Vulnerabilities by Version and Privileges

Supported Database Version ¹	PUBLIC (i.e., APPLSYSPUB)	Other Privileges	No Default Privileges ²
9.2.0.8	DB03 – Core RDBMS DB09 – Net Services DB10 – Core RDBMS DB12 – Export DB13 – DBMS_STATS	DB01 – DBMS_AQ	DB11 – Data Pump
10.1.0.5	DB03 – Core RDBMS DB05 – SDO_UTIL DB06 – SDO_GEOM DB07 – SDO_IDX DB09 – Net Services DB10 – Core RDBMS DB12 – Export DB13 – DBMS_STATS	DB01 – DBMS_AQ DB14 – Fine Grained Auditing DB15 – DBMS_AQJMS_INT	DB02 – DBMS_CDC_UTILITY DB11 – Data Pump
10.2.0.3	DB03 – Core RDBMS DB05 – SDO_UTIL DB06 – SDO_GEOM DB07 – SDO_IDX DB09 – Net Services DB10 – Core RDBMS DB12 – Export DB13 – DBMS_STATS	DB01 – DBMS_AQ DB14 – Fine Grained Auditing	DB02 – DBMS_CDC_UTILITY DB11 – Data Pump

¹ Only Oracle Applications 11i and R12 certified and CPU supported versions are included.

² 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. Neither Oracle nor any security researchers perform dependency checks to determine if the vulnerability could potentially be exploited through another package.

ORACLE APPLICATION SERVER VULNERABILITIES

ORACLE E-BUSINESS SUITE 11I

None of the Oracle Application Server vulnerabilities affect the Oracle E-Business Suite 11i. There has 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.

ORACLE E-BUSINESS SUITE R12

A single vulnerability, AS04, impacts the Oracle E-Business Suite R12 application servers. This vulnerability is in the Dynamic Monitoring Service (DMS) component.

JINITIATOR VULNERABILITIES (11I ONLY)

A new vulnerability in Jinitiator 1.3.1 in version 1.3.1.14 and prior has been fixed as part of the April 2008 CPU. Two vulnerabilities impacting Jinitiator 1.1.8.x and 1.3.1.x., which were previously published in September 2007 and more information is available [here](#), were fixed as part of the January 2008. As part of the January 2008 CPU, Jinitiator should have been upgraded to 1.3.1.29, which is not vulnerable. If Jinitiator was not upgraded already to 1.3.1.29, then it should be upgraded as part of the April 2008 patching.

It is very important all previous Jinitiator 1.1.8.x and 1.3.1.x versions are removed from the client. When Jinitiator is installed, the new version is installed in a separate directory and does not overwrite any previous versions. All previous installations are fully accessible and exploitable, therefore, they must be either removed or have the kill-bit set to stop possible execution (see Metalink Note ID 124606.1 for more information).

This vulnerability only impacts Oracle E-Business Suite 11i since Jinitiator is not certified with R12 and instead the Sun Java Plug-in is used.

ORACLE E-BUSINESS SUITE 11I AND R12 VULNERABILITIES

Vulnerabilities: APP01 – APP11

APP01, APP02, APP03, APP09, APP10 – ORACLE ADVANCED PRICING [11I AND R12]

Multiple high-risk vulnerabilities in Advanced Pricing test servlets, which are not normally used.

APP04 – APPLICATION OBJECT LIBRARY (AOL/FND) [11I AND R12]

A database denial of service (DoS) issue in a test web page, which should only be accessed by administrators for testing OA Framework and Self-Service.

APP05 – ORACLE APPLICATIONS FRAMEWORK (OA FRAMEWORK) [11I]

An information disclosure issue in a test servlet, which is not normally used.

APP06 – ORACLE APPLICATIONS MANAGER (OAM) [11I AND R12]

An information disclosure issue caused when OAM debugging and logging is enabled.

APP07 – APPLICATION OBJECT LIBRARY (AOL/FND) [11I AND R12]

A cross site scripting (XSS) issue in a standard utility type AOL web page.

APP08 – ORACLE APPLICATIONS TECHNOLOGY STACK (TXK) [11I AND R12]

A mis-configuration in the JTF Fulfillment Server, which may result in an information disclosure.

APP11 – APPLICATION OBJECT LIBRARY (AOL/FND) [11I AND R12]

A security bug that may potentially allow unauthorized access to Concurrent Manager output and logs, although, a valid session is required to exploit this vulnerability.

Note: 8 of the 11 security bugs fixed this quarter were discovered by Integrigy and reported to Oracle in November 2007.

11I PATCH ANALYSIS

For the Oracle E-Business Suite 11i, install the patches as specified in Section 2 of [Oracle Metalink Note ID Note 557157.1](#) "Oracle E-Business Suite Critical Patch Update Note April 2008". You should also review the pre-installation notes for the Oracle Database and Oracle Application Server prior to installing those patches.

11I 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, 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.H 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 April 2008 CPU, ATG_PF.H RUP5 or RUP6 is required.

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 January 2008 CPU and prior CPUs, the following technology stack upgrades may be required –

- If ATG_PF.H RUP4 is installed, RUP5 or RUP6 must be installed
- If the database version is 10.2.0.2 is installed, the 10.2.0.3 patchset 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 April 2008 CPU –

Release	Database	App Server (Apache)	Developer	JInitiator (Windows 2000/XP)	FND.x	ATG_PF
11.5.1 – 11.5.8	<i>Desupported</i>					
11.5.9	<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 <i>10.2.0.2</i> 10.2.0.3	<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 – 25</i> 1.1.8.27 <i>1.3.1.9 – 28</i> 1.3.1.29	<i>FND.G*</i> FND.H	11i.ATG_PF.H and (11i.ATG_PF.H RUP5 or 11i.ATG_PF.H RUP6)
11.5.10	<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 <i>10.2.0.2</i> 10.2.0.3	<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> 1.1.8.27 <i>1.3.1.18*</i> <i>1.3.1.21-28</i> 1.3.1.29	FND.H*	11i.ATG_PF.H RUP5 or 11i.ATG_PF.H RUP6
11.5.10.2	<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 <i>10.2.0.2</i> 10.2.0.3	<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> 1.1.8.27 <i>1.3.1.18*</i> <i>1.3.1.21-28</i> 1.3.1.29	FND.H*	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.

11I ORACLE DATABASE PATCHES

The database portion of the patch fixes 13 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 thirteen CPUs (January 2005 through January 2008) 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 update (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.

11I 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
1.1.8	1.1.8.27	1.1.8.27
1.3.1	1.3.1.29	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 11I PATCHES

All implementations will be required to apply five 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
6831988	High	High	<p>Oracle Applications Technology Stack (TXK)</p> <ul style="list-style-type: none"> APPO5, APPO6, and APPO8 are fixed in this patch through updating of AutoConfig templates and all are information disclosure issues. This patch is a subset of a standard TXK AutoConfig RUP (about 25%), although, only a few files are updated. ATG_PF.H RUP5 includes 5759055 "TXK AutoConfig Rollup Patch P (Mar/Apr 2007)". A comparison of this patch with AutoConfig RUP P shows 9 template files or AutoConfig scripts are updated. If 5985992 "TXK AutoConfig Rollup Patch Q (Jul/Aug 2007)" is applied, 6 template files or AutoConfig scripts are updated. Testing is dependent on the last TXK AutoConfig Rollup patch and ATG_PF.H Rollup patch applied. The ATG_PF.H RUPs include the AutoConfig RUPs, so ATG_PF.H RUP6 includes AutoConfig RUP R. Due to versioning, the older the AutoConfig RUP, then the more testing. Mandatory for all implementations All 3 vulnerabilities are blocked by the URL Firewall for external access
6858005	Low	Low	<p>Oracle Application Object Library (AOL)</p> <ul style="list-style-type: none"> A database denial of service (DoS) in an AOL diagnostics web page and no authentication is required No testing required Mandatory for all implementations Blocked by the URL Firewall for external access
6858550	Medium	Low	<p>Oracle Application Object Library (AOL)</p> <ul style="list-style-type: none"> Cross-site scripting (XSS) in standard utility web page No testing required Mandatory for all implementations Blocked by the URL Firewall for external access
6802774	Low	Low	<p>Oracle Application Object Library (AOL)</p> <ul style="list-style-type: none"> Potential unauthorized access to Concurrent Manager output and log files A valid Oracle Applications session is required Basic testing of viewing Concurrent Manager output Mandatory for all implementations Blocked by the URL Firewall for external access
6810748	High	Low	<p>Advanced Pricing (QP)</p> <ul style="list-style-type: none"> Multiple vulnerabilities in Advanced Pricing test servlets No testing required Mandatory for all implementations Blocked by the URL Firewall for external access

R12 PATCH ANALYSIS

For the Oracle E-Business Suite R12, install the patches as specified in section 1 of [Oracle Metalink Note ID Note 557157.1](#) "Oracle E-Business Suite Critical Patch Update Note April 2008". You should also review the pre-installation notes for the Oracle Database and Oracle Application Server prior to installing those patches.

R12 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 and Application Server. 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.

For the April 2008 CPU, the following technology stack upgrades may be required –

- Oracle Database version upgrade from 10.2.0.2 to 10.2.0.3
- Oracle Application Server version upgrade from 10.1.3.0.0 to 10.1.3.3.0 (Metalink Note ID [454811.1](#))

ORACLE DATABASE PATCHES

The database portion of the patch fixes 13 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 April 2008 patch includes all fixes for the previous 10.2.0.3 CPUs (January 2007 through January 2008).

TESTING

An abbreviated testing cycle should be performed similar to testing for a minor database update (e.g., 10.2.0.2 to 10.2.0.3). 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

The R12 architecture includes two installations of Oracle Application Server and thus requires 2 different Application Server CPU patches. Since the application server patches are cumulative, all previous security will also be applied.

TESTING

If previous CPU patches have been applied, only minimal testing should be required as the only fix affecting Oracle E-Business Suite is to the Dynamic Monitoring Service (DMS). Where previous CPUs application server security have not been applied, additional testing will be required and is dependent on the number of CPU patches not applied.

ORACLE E-BUSINESS SUITE R12 PATCHES

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. The single patch includes both technology stack security fixes as well as functional module security fixes. Since the patch is cumulative, changes to AP, Benefits, HR, Payroll, Business Intelligence, iPayment, Localizations, Quoting, etc. are also included from previous CPUs. The exact testing required is dependent on the last R12 CPU patch applied.

An important change for the April 2008 CPU is that there is no concurrent release of a R12 RUP (i.e., 12.0.5) and potentially there will be no additional 12.0 RUPs.

Importance	Patch Risk	Notes
Medium	Low	Oracle Applications Technology Stack (TXK) <ul style="list-style-type: none"> ▪ APP06 and APP08 are fixed through updating of AutoConfig templates and all are information disclosure issues ▪ Only 4 AutoConfig templates and control files are update with minimal to no risk of impact to the application ▪ No testing required ▪ Both vulnerabilities are blocked by the URL Firewall for external access
Low	Low	Oracle Application Object Library (AOL) <ul style="list-style-type: none"> ▪ A database denial of service (DoS) in an AOL diagnostics web page and no authentication is required ▪ No testing required ▪ Blocked by the URL Firewall for external access
Medium	Low	Oracle Application Object Library (AOL) <ul style="list-style-type: none"> ▪ Cross-site scripting (XSS) in standard utility web page ▪ No testing required ▪ Mandatory for all implementations ▪ Blocked by the URL Firewall for external access
Low	Low	Oracle Application Object Library (AOL) <ul style="list-style-type: none"> ▪ Potential unauthorized access to Concurrent Manager output and log files ▪ A valid Oracle Applications session is required ▪ Basic testing of viewing Concurrent Manager output ▪ Blocked by the URL Firewall for external access
High	Low	Advanced Pricing (QP) <ul style="list-style-type: none"> ▪ Multiple vulnerabilities in Advanced Pricing test servlets ▪ No testing required ▪ Blocked by the URL Firewall for external access

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.

11i 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 8 of [Oracle Metalink Note ID 552248.1](#) for the exact patch for your version of the Oracle Database.

NEXT SCHEDULED DOWNTIME

2. 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

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

11i 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 8 of [Oracle Metalink Note ID 552248.1](#) 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. A database patchset may have to be applied if the current database version is not supported by the CPU.
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 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 technology stack 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 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.

R12 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 R12 (12.0.0 to 12.0.4).

AS SOON AS POSSIBLE

1. Apply the Oracle Database security patch as soon as possible. See Table 8 of [Oracle Metalink Note ID 552248.1](#) for the exact patch for your version of the Oracle Database.

NEXT SCHEDULED DOWNTIME

2. Apply the Oracle E-Business Suite R12 cumulative patch. See the above table for necessary testing requirements.

NEXT SCHEDULE DOWNTIME OR UPGRADE CYCLE

3. Apply the Oracle Application Server 10.1.2 and 10.1.3 security patches.

R12 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 R12 (12.0.0. to 12.0.4) and the exact patches will be dependent on 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 April 2008 security patch. See Table 8 of [Oracle Metalink Note ID 552248.1](#) 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. A database patchset may have to be applied if the current database version is 10.2.0.2.
2. Apply the Oracle E-Business Suite R12 cumulative CPU patch for April 2008. See the above table for necessary testing requirements for this quarter. Since this patch is cumulative and includes security fixes for technology stack as well as functional modules, functional testing is required depending on the number of CPU patches missing. An alternative is to apply the January 2008 12.0.4 R12 Rollup and then the April 2008 CPU patch.

NEXT SCHEDULE EXTENDED DOWNTIME OR UPGRADE CYCLE

3. Apply the Oracle Applications Server 10.1.2 and 10.1.3 CPU patches from April 2008. These patches are cumulative.

REFERENCES

CRITICAL PATCH UPDATE

- Oracle Critical Patch Update April 2008 Advisory, 15 April 2008, <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html>

ORACLE DATABASE

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 15 April 2008, [Oracle Metalink Note ID 552248.1](#)
- 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 April 2008, [Oracle Metalink Note ID 552248.1](#)

ORACLE E-BUSINESS SUITE

- Oracle Critical Patch Update April 2008 Pre-Installation Note for Oracle E-Business Suite, 15 April 2008, [Oracle Metalink Note ID Note 557157.1](#)
- Prior E-Business Suite Security Alerts, 25 March 2008, [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, 3 March 2008, [Oracle Metalink Note ID 363827.1](#)
- Integrity, Oracle Jinitiator 1.1.8 Vulnerability, 11 September 2007, <http://www.integrity.com/oracle-security-blog/oracle-jinitiator-vulnerability>

HISTORY

April 21, 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 – April 2008.

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

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.