Subject: **Oracle Critical Patch Update January 2007 Advisory**

Doc ID: **Note:403335.1** Type: **REFERENCE**

Last Revision Date: **16-JAN-2007** Status: **PUBLISHED**

Oracle Critical Patch Update - January 2007

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. It also includes non-security fixes that are required (because of interdependencie security patches. This Critical Patch Update contains 51 new security fixes across all products.

Supported Products and Components Affected

Security vulnerabilities addressed by this Critical Patch Update affect the products listed in the categories below. The product area of the patches for the listed versio in [square brackets] following the product versions. Please click on the link in [square brackets] or in the Patch Availability Table to access the documentation for thos

Category I

Product releases and versions that are in Premier Support or Extended Support, under the Oracle Lifetime Support policy; or Error Correction Support (ECS) or Exte Maintenance Support (EMS), under the previous support policy:

• Oracle Database 10*g* Release 2, versions 10.2.0.1, 10.2.0.2, 10.2.0.3	[Database]
• Oracle Database 10*g* Release 1, versions 10.1.0.4, 10.1.0.5	[Database]
• Oracle9*i* Database Release 2, versions 9.2.0.7, 9.2.0.8	[Database]
• Oracle Identity Management 10*g*, version 10.1.4.0.1	[Application Server]
• Oracle Application Server 10*g* Release 3, versions 10.1.3.0.0, 10.1.3.1.0	[Application Server]
• Oracle Application Server 10*g* Release 2, versions 10.1.2.0.0 - 10.1.2.0.2, 10.1.2.1.0, 10.1.2.2.0	[Application Server]
• Oracle Application Server 10*g* (9.0.4), versions 9.0.4.2, 9.0.4.3	[Application Server]
• Oracle E-Business Suite Release 11*i*, versions 11.5.7 - 11.5.10 CU2	[E-Business Suite]
• Oracle E-Business Suite Release 11.0	[E-Business Suite]
• Oracle Enterprise Manager 10*g* Grid Control Release 2, version 10.2.0.1	[Enterprise Manager]
• Oracle Enterprise Manager 10*g* Grid Control Release 1, versions 10.1.0.4, 10.1.0.5	[Enterprise Manager]
• Oracle PeopleSoft Enterprise PeopleTools versions 8.22, 8.47, 8.48	[PeopleSoft/JDE]

Category II

Products and components that are bundled with the products listed in Category I:

- Oracle Developer Suite, versions 9.0.4.3, 10.1.2.0.2 [Developer Suite]

Category III

Products that are de-supported as a standalone installation but are supported when installed with the products listed in Category I:

• Oracle9*i* Database Release 1, versions 9.0.1.5, 9.0.1.5 FIPS	[Application Server]
• Oracle9*i* Database Release 1, version 9.0.1.4	[Collaboration Suite]
• Oracle8*i* Database Release 3, version 8.1.7.4	[E-Business Suite]
• Oracle9*i* Application Server Release 2, version 9.0.2.3	[Collaboration Suite]
• Oracle9*i* Application Server Release 1, version 1.0.2.2	[E-Business Suite]
• Oracle Developer Suite, version 6*i*	[E-Business Suite]

Patches for Category III products are only available when these products are installed as part of Category I products, and are tested solely on supported configuratio environments. Please refer to the documentation for each product for specific details concerning the support and availability of patches.

Category IV

Products that are supported only on selected platforms. Please consult the additional documentation for details.

- Oracle Database 10*g* Release 1, version 10.1.0.3 [Database]
- Oracle9*i* Database Release 2, versions 9.2.0.5, 9.2.0.6 [Database]
- Oracle Application Server 10*g* Release 1 (9.0.4), version 9.0.4.1 [Application Server]
- Oracle Enterprise Manager 10*g* Grid Control Release 1, version 10.1.0.3 [Enterprise Manager]

Patch Availability Table and Risk Matrices

The Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne, JD Edwards One Tools, PeopleSoft Enterprise Portal Applications and PeopleSoft Enterprise PeopleTools patches in the Updates are cumulative; each Critical Patch Update contains from the previous Critical Patch Updates.

Oracle E-Business Suite and Applications patches are not cumulative, so E-Business Suite and Applications customers should refer to previous Critical Patch Updat previous fixes they want to apply.

For each Oracle product being administered, please consult the documentation for patch availability information and installation instructions referenced from the follo For an overview of the Oracle product documentation related to this Critical Patch Update, please refer to the Oracle Critical Patch Update January 2007 Documenta MetaLink Note 405814.1.

Product	Risk Matrix	Pointer to More Information
Oracle Database	Appendix A - Oracle Database Risk Matrix	Critical Patch Update Availability for Oracle Server and Middlew Products, MetaLink Note 403325.1
Oracle Application Server	Appendix B - Oracle Application Server Risk Matrix	Critical Patch Update Availability for Oracle Server and Middlew Products, MetaLink Note 403325.1
Oracle Collaboration Suite	Appendix C - Oracle Collaboration Suite Risk Matrix	Critical Patch Update Availability for Oracle Server and Middlew Products, MetaLink Note 403325.1
Oracle E-Business Suite and Applications	Appendix D - Oracle E-Business Suite and Applications Risk Matrix	E-Business Suite Critical Patch Update Note, MetaLink Note 40
Oracle Enterprise Manager	Appendix E - Enterprise Manager Risk Matrix	Critical Patch Update Availability for Oracle Server and Middlew Products, MetaLink Note 403325.1
Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne	Appendix F - Oracle PeopleSoft and JD Edwards Applications Risk Matrix	Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne A

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly fixed by the patches associated with this advisory. Risk matrices for previous fixes can be found in previo Patch Update advisories.

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. The same vulnerability appears with the same **Vuln #** in all risk matrices. *Italic* vulnerabilities in code included from other product areas.

Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update (CPU) or a Security Alert. Results of the security analysis are reflecte associated documentation describing, for example, the type of vulnerability, the conditions required to exploit it and the result of a successful exploit. Oracle provides information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. As a matter of policy, Oracle does not disc detailed information about an exploit condition or results that can be used to conduct a successful exploit. Oracle will not provide additional information about the spe vulnerabilities beyond what is provided in the CPU or Security Alert notification, the Patch Availability Matrix, the readme files, and FAQs. Oracle does not provide ad notification on CPU or Security Alerts to individual customers. Finally, Oracle does not distribute exploit code nor “proof-of-concept” code for vulnerabilities in our pro

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that fixes are applied as soon as possible. Depending on your environment, it may be p reduce the risk of successful attack by restricting network protocols required by an attack. For attacks that require certain privileges or access to certain packages, re privileges or the ability to access the packages from untrusted users may help reduce the risk of successful attack. Both approaches may break application functiona Oracle strongly recommends changes are tested on non-production systems. Neither approach should be considered a long term solution as neither corrects the unc problem.

Unsupported Products and De-Supported Versions

Unsupported products, releases and versions are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that earlie of affected releases are also affected by these vulnerabilities.

Supported products are patched in accordance with the Critical Patch Update policy summarized in the CPU Frequently Asked Questions document linked from the F section.

Critical Patch Update patches are available for customers who have purchased Extended Maintenance Support (EMS) before the implementation of the Lifetime Sup De-support Notices indicate whether EMS is available for a particular release and platform, as well as the specific period during which EMS will be available.

Customers with valid licenses for product versions covered by Extended Support (ES), before the implementation of the Lifetime Support Policy, are entitled to down existing fixes; but new issues that may arise from the application of patches are not covered under ES. Therefore, ES customers should have comprehensive plans t removal of any applied patch.

Critical Patch Update patches are not provided for product versions which are no longer covered under the Extended Maintenance Support plan or the Lifetime Supp We recommend that customers upgrade to the latest supported version of Oracle products in order to obtain patches.

Please review the "Extended Support" section within the Technical Support Policies for further guidelines regarding ES and EMS.

Credits

The following people discovered and brought security vulnerabilities addressed by this Critical Patch Update to Oracle's attention: Andy Davis of Information Risk Ma Plc; Vicente Aguilera Diaz of Internet Security Auditors, S.L.; Esteban Martinez Fayo of Application Security, Inc.; Tony Fogarty of BT Global Services; Oliver Karow Symantec; Joxean Koret; Alexander Kornbrust of Red Database Security GmbH; David Litchfield and Mark Litchfield of Next Generation Security Software Ltd.; and ratty.

Critical Patch Update Schedule

Critical Patch Updates are released on the Tuesday closest to the 15th day of January, April, July and October. The next four dates are:

- 17 April 2007
- 17 July 2007
- 16 October 2007
- 15 January 2008

References

- Oracle Critical Patch Updates and Security Alerts main page [Oracle Technology Network]
- Oracle PeopleSoft Security main page [Customer Connection]
- Critical Patch Update - January 2007 Documentation Map [MetaLink Note 405814.1]
- Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions [MetaLink Note 360470.1]
- Common Vulnerability Scoring System (CVSS) Risk Matrix definitions [MetaLink Note 394486.1] [Customer Connection]
- Use of Common Vulnerability Scoring System (CVSS) by Oracle [MetaLink Note 394487.1] [Customer Connection]
- List of public vulnerabilities fixed in Critical Patch Updates and Security Alerts [Oracle Technology Network]

Modification History

2007-JAN-16	Initial release

Appendix A - Oracle Database

Oracle Database Executive Summary

This Critical Patch Update contains a total of 26 new security fixes for Oracle Database products, divided as follows:

- 17 new security fixes for the Oracle Database, 1 of which may be remotely exploitable without authentication, i.e. it may be exploited over a network without the username and password. 1 fix is applicable to Oracle Database client-only installations, i.e. installations that do not have the Oracle Database installed.
- 9 new security fixes for Oracle HTTP Server, 8 of which may be remotely exploitable without authentication, i.e. they may be exploited over a network without th a username and password. Oracle HTTP Server is an optional product that is **not** installed by default with the Oracle Database. If it has not been installed, this not be present and the Oracle HTTP Server patches are not required. Oracle Database versions up to and including Oracle Database 9*i* Release 2 allowed Ora Server to be installed as an optional component of the database. Oracle Database versions 10*g* Release 1 and higher include Oracle HTTP Server on the Com
- There are no new security fixes for Oracle Application Express (formerly called HTML DB), but versions up to and including version 2.0 should be upgraded to t version. Oracle Application Express is an optional product that is **not** installed with the Oracle Database. If it has not been installed (it is provided on the Compa the Oracle Database CD set for some Oracle Database versions), this software will not be present and the patches are not required.
  Please refer to Appendix A in the October 2006 Critical Patch Update advisory for more information.

Oracle Database Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
DB01	Advanced Queuing	Oracle Net	Execute on sys.dbms_aq	No	2.8	Remote	Low	Required	Partial	Partial	None	9*i*
DB02	Change Data Capture	Oracle Net	Execute on sys.dbms_cdc_subscribe	No	2.8	Remote	Low	Required	Partial	Partial	None	9*i*R2
DB03	Data Guard	Oracle Net	Execute on sys.dbms_drs	No	2.8	Remote	Low	Required	None	Partial	Partial+	9*i*R2
DB04	Log Miner	Oracle Net	Execute on sys.dbms_log_mnr	No	2.8	Remote	Low	Required	None	Partial	Partial	9*i*

DB05	Oracle Spatial	Oracle Net	Execute on mdsys.md	No	2.8	Remote	Low	Required	None	Partial	Partial+	8*i*
DB06	XMLDB	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9*i*
DB07	Advanced Replication	Oracle Net	Execute on sys.dbms_repcat_untrusted	No	1.4	Remote	Low	Required	None	None	Partial+	9*i*
DB08	Export	Oracle Net	Execute on sys.dbms_logrep_util	No	1.4	Remote	Low	Required	None	None	Partial	9*i*R2
DB09	Oracle Streams	Oracle Net	Execute on sys.dbms_capture_adm_internal	No	1.4	Remote	Low	Required	None	None	Partial	9*i*R2
OWF01	Oracle Workflow Cartridge	HTTP	Valid session	No	1.4	Remote	Low	Required	None	Partial	None	9*i*R2
DB10	Advanced Security Option	Local	Ability to run oklist or okdstry programs	No	0.0	Local	Low	Required	None	None	None	8*i*
DB11	Export	Local	Ability to run expdp or impdp programs	No	0.0	Local	Low	Required	None	None	None	10*g*
DB12	NLS Runtime	Local	Ability to run lmsgen program	No	0.0	Local	Low	Required	None	None	None	8*i*
DB13	Oracle Net Services	Local	Ability to run tnslsnr program	No	0.0	Local	Low	Required	None	None	None	8*i*
DB14	Oracle Text	Local	Ability to run ctxkbtc program	No	0.0	Local	Low	Required	None	None	None	8*i*
DB15	Oracle Text	Local	Ability to run ctxload program	No	0.0	Local	Low	Required	None	None	None	9*i*
DB16	Recovery Manager	Local	Ability to run oklist program	No	0.0	Local	Low	Required	None	None	None	8*i*

Notes:

- Vulnerabilities with a CVSS *base score* of 0.0 represent problems that are not exploitable in a default database environment. If custom code runs affected progr privileged user, it may allow malicious code to be run as that user.
- Oracle Database version 10.2.0.3 has recently been released and it has tentatively been added to the risk matrix. Definitive information on the impact of vulnera this version will be provided in an update to this advisory. This will happen when the Critical Patch Update patches for version 10.2.0.3 are released.

Oracle Database Client-only Installations

One new database vulnerability addressed by this Critical Patch Update, DB11, affects Oracle Database client-only installations (installations that do not have the Or Database installed). It is potentially exploitable where a privileged operating system process is passing input from an untrusted source to the affected program. Oracl recommends applying this Critical Patch Update to client-only installations which may be using the affected program in this way, or which are affected by client-only i in prior Critical Patch Updates if the prior patches have not been applied.

Client-side software in the middle tier is patched as part of the general middle tier patch and customers do not need to apply additional patches. Exceptions will be d in the Patch Availability Document for Oracle Server and Middleware Products, or the Pre-Installation Note, depending on the product.

Oracle HTTP Server Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
OHS01	Oracle HTTP Server	HTTPS	SSL Module	Yes	7.0	Remote	Low	Not Required	Partial	Partial	Partial	9*i*
	Oracle HTTP											

OHS02	Oracle HTTP Server	HTTPS	SSL Module	Yes	5.6	Remote	High	Not Required	Partial	Partial	Partial	9*i*
OPMN01	Oracle Process Mgmt & Notification	ONS	None	Yes	4.7	Remote	Low	Not Required	None	Partial	Partial	9*i*
OHS03	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9*i*
OHS04	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9*i*
OHS05	Oracle HTTP Server	HTTPS	SSL Module	Yes	2.3	Remote	Low	Not Required	None	None	Partial	9*i*
OHS06	Oracle HTTP Server	HTTPS	SSL Module	Yes	2.3	Remote	Low	Not Required	None	None	Partial	9*i*
OHS07	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial	None	None	9*i*
OPMN02	Oracle Process Mgmt & Notification	ONS	None	No	2.0	Local	Low	Required	Partial	Partial	None	9*i*

Appendix B - Oracle Application Server

Oracle Application Server Executive Summary

This Critical Patch Update contains 12 new security fixes for Oracle Application Server, 8 of which may be remotely exploitable without authentication, i.e. they may b over a network without the need for a username and password. No new fixes are applicable to client-only installations, i.e. installations that do not have Oracle Applic Server installed.

This Critical Patch Update also contains 8 new security fixes for Oracle Application Server products that are not supported for standalone use, but are supported for of supported products, i.e. those listed in the Category I section. More details of these fixes can be found in the sections of this document covering: Oracle Database Collaboration Suite and Oracle E-Business Suite. They are not discussed further in this section, as they do not apply to Oracle Application Server standalone instanc

Oracle Application Server products that are bundled with the Oracle Database are affected by the vulnerabilities listed in the Oracle Database section. They are not c further in this section and are not listed in the Oracle Application Server risk matrix.

Oracle Application Server Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
OPMN01	Oracle Process Mgmt & Notification	ONS	None	Yes	4.7	Remote	Low	Not Required	None	Partial	Partial	9.0.4.1
OC4J02	Oracle Containers for J2EE	HTTP	None	Yes	3.7	Remote	High	Not Required	Partial	Partial	None	9.0.4.1
OC4J03	Oracle Containers for J2EE	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial+	None	None	9.0.4.1
OC4J04	Oracle Containers for J2EE	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4.1
OHS03	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4.1
OHS04	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4.1

REP01	Oracle Reports Developer	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4.1
OPMN02	Oracle Process Mgmt & Notification	ONS	None	No	2.0	Local	Low	Required	Partial	Partial	None	9.0.4.1
OC4J07	Oracle Containers for J2EE	HTTP	Valid Session	Yes	1.9	Remote	High	Not Required	Partial	None	None	10.1.2.0.0
OWF01	Oracle Workflow Cartridge	HTTP	Valid session	No	1.4	Remote	Low	Required	None	Partial	None	9.0.4.3
OC4J08	Oracle Containers for J2EE	Local	Ability to run jazn.jar	No	1.0	Local	Low	Required	Partial	None	None	9.0.4.1
OID01	Oracle Internet Directory	LDAP	Local	No	1.0	Local	Low	Required	Partial	None	None	10.1.4.0

Notes:

- OC4J03 requires manual steps to be performed. Details can be found in the Patch Availability Document for Oracle Server and Middleware Products, MetaLink 403325.1.

Oracle Application Server Client-only Installations

No new vulnerabilities addressed by this Critical Patch Update affect client-only installations of Application Server products. However, fixes for Oracle Containers for Oracle Reports Developer which affect client-only installations were released in the October 2006 Critical Patch Update. Please refer to the October 2006 Critical Pat advisory for more information if these patches have not yet been applied.

Appendix C - Oracle Collaboration Suite

Oracle Collaboration Suite Executive Summary

There are no new Oracle Collaboration Suite specific fixes in this Critical Patch Update. Please refer to the July 2006 Critical Patch Update for the latest Oracle Colla Suite specific fixes.

This Critical Patch Update contains 14 Oracle Application Server vulnerabilities that are in code included in Oracle Collaboration Suite. 11 of these vulnerabilities may remotely exploitable without authentication, i.e. they may be exploited over a network without the need for a username and password. The application tier stack patch as part of this Critical Patch Update contains these fixes and should be installed on Oracle Collaboration Suite instances.

Oracle Collaboration Suite bundles the Oracle Database. All the fixes listed in the Oracle Database part of the Oracle Database section are applicable. The Oracle C Suite documentation referenced from this advisory lists the patches that should be installed on Oracle Collaboration Suite instances to fix these Oracle Database issu

Oracle Collaboration Suite Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
OPMN01	Oracle Process Mgmt & Notification	ONS	None	Yes	4.7	Remote	Low	Not Required	None	Partial	Partial	9.0.4
OC4J01	Oracle Containers for J2EE	HTTP	None	Yes	4.7	Remote	Low	Not Required	Partial	Partial	None	9.0.4
OC4J02	Oracle Containers for J2EE	HTTP	None	Yes	3.7	Remote	High	Not Required	Partial	Partial	None	9.0.4
OC4J03	Oracle Containers for J2EE	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial+	None	None	9.0.4
OC4J04	Oracle Containers for J2EE	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4
OC4J05	Oracle Containers for	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial	None	None	9.0.4

	J2EE											
OC4J06	Oracle Containers for J2EE	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4
OHS03	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4
OHS04	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4
REP01	Oracle Reports Developer	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	9.0.4
OPMN02	Oracle Process Mgmt & Notification	ONS	None	No	2.0	Local	Low	Required	Partial	Partial	None	9.0.4
OC4J07	Oracle Containers for J2EE	HTTP	Valid Session	Yes	1.9	Remote	High	Not Required	Partial	None	None	10.1.2
OWF01	Oracle Workflow Cartridge	HTTP	Valid session	No	1.4	Remote	Low	Required	None	Partial	None	10.1.2
OC4J08	Oracle Containers for J2EE	Local	Ability to run jazn.jar	No	1.0	Local	Low	Required	Partial	None	None	9.0.4

Appendix D - Oracle E-Business Suite and Applications

Oracle E-Business Suite and Applications Executive Summary

This Critical Patch Update contains 7 new security fixes for the Oracle E-Business Suite, including one in Oracle Workflow Cartridge. None of these vulnerabilities ma remotely exploited without authentication.

Oracle E-Business Suite includes Oracle9*i* Application Server Release 1, version 1.0.2.2 code, including Oracle Reports Developer. 6 Oracle Application Server vuln are applicable to this version of the code, and all may be remotely exploitable without authentication, i.e. they may be exploited over a network without the need for a and password. The application tier stack patch supplied as part of this Critical Patch Update contains these fixes and should be installed on Oracle E-Business Suite

Oracle E-Business Suite products include an Oracle Database which is affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle E Suite products is dependent on the Oracle Database version being used. Oracle Database vulnerabilities are not listed in the Oracle E-Business Suite risk matrix, bu patched.

There are no new security fixes specific to Oracle Life Sciences Applications (previously known as Oracle Pharmaceutical Applications).

Oracle Life Sciences Applications includes Oracle Application Server components which should be patched. The exposure of Oracle Life Sciences Applications depe version of Oracle Application Server being used. The E-Business Suite risk matrix includes Oracle Application Server vulnerabilities applicable to Oracle9*i* Applicatio Release 1, version 1.0.2.2, and the Oracle Application Server section lists vulnerabilities applicable to other versions.

Oracle Life Sciences Applications includes Oracle Database software which is affected by the vulnerabilities listed in the Oracle Database section. The exposure of O Sciences Applications is dependent on the Oracle Database version being used. Oracle Database vulnerabilities are not listed in the Oracle Life Sciences Applicatio matrix, but should be patched.

Oracle Life Sciences Applications customers should refer to MetaLink Note 403803.1 for detailed information on installing Oracle Application Server and Oracle Data security patches.

Oracle E-Business Suite Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
OHS01	Oracle HTTP Server	HTTPS	SSL Module	Yes	7.0	Remote	Low	Not Required	Partial	Partial	Partial	11.0
OHS02	Oracle HTTP Server	HTTPS	SSL Module	Yes	5.6	Remote	High	Not Required	Partial	Partial	Partial	11.0
OHS05	Oracle HTTP Server	HTTPS	SSL Module	Yes	2.3	Remote	Low	Not Required	None	None	Partial	11.0
OHS06	Oracle HTTP	HTTPS	SSL Module	Yes	2.3	Remote	Low	Not Required	None	None	Partial	11.0

OHS06	Server	HTTPS	SSL Module	Yes	2.3	Remote	Low	Not Required	None	None	Partial	11.0
OHS07	Oracle HTTP Server	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial	None	None	11.0
REP01	Oracle Reports Developer	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	11.5.7
APPS01	Oracle Application Object Library	HTTP	System Administrator	No	1.6	Local	High	Required	Partial	Partial	None	11.5.7
OWF01	Oracle Workflow Cartridge	HTTP	Valid session	No	1.4	Remote	Low	Required	None	Partial	None	11.5.7
APPS02	Oracle Exchange	HTTP	Negotiations User	No	1.4	Remote	Low	Required	Partial	None	None	6.2.3
APPS03	Oracle Human Resources	HTTP	Human Resource Administrator	No	1.4	Remote	Low	Required	Partial	None	None	11.5.7
APPS04	Oracle Payables	HTTP	Oracle Payables User	No	1.4	Remote	Low	Required	Partial	None	None	11.5.7
APPS05	Oracle Trading Community Architecture	HTTP	Trading Community Administrator	No	1.4	Remote	Low	Required	Partial	None	None	11.5.7
APPS06	Oracle Web Applications Desktop Integrator	HTTP	Desktop Integration Responsibility	No	1.4	Remote	Low	Required	None	Partial	None	11.5.7

Appendix E - Oracle Enterprise Manager

Oracle Enterprise Manager Executive Summary

This Critical Patch Update contains 6 new security fixes for Oracle Enterprise Manager, 5 of which may be remotely exploitable without authentication, i.e. they may b over a network without the need for a username and password.

Oracle Enterprise Manager includes Oracle Database and Oracle Application Server components which are affected by the vulnerabilities listed in the Oracle Databa Oracle Application Server sections. The Oracle Database and Oracle Application Server vulnerabilities that affect a particular instance of Oracle Enterprise Manager the Oracle Database and Oracle Application Server versions in use. Refer to the risk matrices in the appropriate sections of this document for more information. The Patch Update includes patches for Oracle Database and Oracle Application Server that can be installed to Oracle Enterprise Manager environments, and these patch be installed.

Oracle Enterprise Manager Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see 394486.1)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
EM01	Oracle Agent	HTTP	None	Yes	7.0	Remote	Low	Not Required	Partial	Partial	Partial	10*g*
EM02	Oracle Agent	HTTP	None	Yes	7.0	Remote	Low	Not Required	Partial	Partial	Partial	10*g*
EM03	Oracle Agent	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial	None	None	10*g*
EM04	Enterprise Manager Console	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	Partial	None	10*g*
EM05	Enterprise Manager Console	HTTP	None	Yes	2.3	Remote	Low	Not Required	Partial+	None	None	10*g*
EM06	Database Cloning & Data Guard Management	HTTP	Valid operating system account	No	1.0	Local	Low	Required	Partial	None	None	10*g*R2

Appendix F - Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne

Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne Executive Summary

This Critical Patch Update contains 3 new security fixes for Oracle PeopleSoft Enterprise PeopleTools, 1 of which may be remotely exploitable without authentication be exploited over a network without the need for a username and password.
There are no new security fixes for Oracle Enterprise Portal Solutions and JD Edwards EnterpriseOne. The security patches released as part of the October 2006 Cri Update should be applied if this has not been done. Please refer to Appendix A in the October 2006 Critical Patch Update advisory for more information.

Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS RISK (see Customer Connection)							Earliest Supported Release Affected
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
PSE01	PeopleTools	HTTP	None	Yes	2.3	Remote	Low	Not Required	None	None	Partial+	8.22 GA 8.47 GA
PSE02	PeopleTools	HTTP	None	No	1.6	Local	Low	Not Required	Partial	None	None	8.22 GA 8.47 GA 8.48 GA
PSE03	PeopleTools	HTTP	Valid Session	No	1.4	Remote	Low	Required	None	Partial	None	8.47 GA 8.48 GA

.