ORACLE

Critical Patch Update - April 2005

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 interdependencies) by those security patches. The Oracle Database Server, Enterprise Manager, and the Oracle Application Server patches in the Updates are cumulative; each successive Critical Patch Update contains the fixes from the previous Critical Patch Updates.

Supported Products Affected

The following supported product releases and versions are affected by the security vulnerabilities addressed by this Critical Patch Update:

- Oracle Database 10*g* Release 1, versions 10.1.0.2, 10.1.0.3, 10.1.0.3.1, 10.1.0.4 (10.1.0.3.1 is supported for Oracle Application Server only)
- Oracle9*i* Database Server Release 2, versions 9.2.0.5, 9.2.0.6
- Oracle9*i* Database Server Release 1, versions 9.0.1.4, 9.0.1.5, 9.0.4 (9.0.1.5 FIPS) (all of which are supported for Oracle Application Server only)
- Oracle8*i* Database Server Release 3, version 8.1.7.4
- Oracle Application Server 10*g* Release 2 (10.1.2)
- Oracle Application Server 10*g* (9.0.4), versions 9.0.4.0, 9.0.4.1
- Oracle9*i* Application Server Release 2, versions 9.0.2.3, 9.0.3.1
- Oracle9*i* Application Server Release 1, version 1.0.2.2
- Oracle Collaboration Suite Release 2, versions 9.0.4.1, 9.0.4.2
- Oracle E-Business Suite and Applications Release 11*i*, versions 11.5.0 through 11.5.10
- Oracle E-Business Suite and Applications Release 11.0
- Oracle Enterprise Manager Grid Control 10*g*, versions 10.1.0.2, 10.1.0.3
- Oracle Enterprise Manager versions 9.0.4.0, 9.0.4.1
- PeopleSoft EnterpriseOne Applications, versions 8.9 SP2 and 8.93
- PeopleSoft OneWorldXe/ERP8 Applications, versions SP22 and higher

Unsupported Products

Unsupported products, releases and versions have neither been tested for the presence of vulnerabilities addressed by this Critical Patch Update, nor patched, in accordance with section 4.3.3.3 of the Software Error Correction Support Policy (MetaLink Note 209768.1). However, it is likely that earlier patch set levels of the affected releases are affected by these vulnerabilities.

Oracle Database Client-only installations

The new database vulnerabilities addressed by this Critical Patch Update do not affect Oracle Database Client-only

installations (installations that do not have the Oracle Database Server installed). Therefore, it is not necessary to apply this Critical Patch Update to client-only installations if a prior Critical Patch Update, or Alert 68, has already been applied to the client-only installations.

Patch Availability and Risk Matrices

For each Oracle product that is being administered, please consult the associated Pre-Installation Note for patch availability information and installation instructions. For an overview of all the documents related to this Critical Patch Update, please see the Oracle Critical Patch Update Documentation Map, MetaLink Note 304410.1.

Product	Risk Matrix	Pre-Installation Note
Oracle Database Server	Appendix A - Oracle Database Server Risk Matrix	Pre-Installation Note for the Oracle Database Server, MetaLink Note 301045.1
Oracle Application Server	Appendix B - Oracle Application Server Risk Matrix	Pre-Installation Note for the Oracle Application Server, MetaLink Note 301046.1
Oracle Collaboration Suite	Appendix C - Oracle Collaboration Suite Risk Matrix	Pre-Installation Note for the Oracle Collaboration Suite, MetaLink Note 301047.1
Oracle E-Business and Applications	Appendix D - Oracle E-Business Risk Matrix	Pre-Installation Note for the Oracle E-Business Suite, MetaLink Note 301048.1
Oracle Enterprise Manager Grid Control	Appendix E - Oracle Enterprise Manager Grid Control Risk Matrix	Pre-Installation Note for the Oracle Enterprise Manager Grid Control, MetaLink Note 301049.1
Oracle PeopleSoft Applications	Appendix F - Oracle PeopleSoft Applications Risk Matrix	PeopleSoft Advisory

Risk Matrix Contents

The risk matrices in this advisory list only the vulnerabilities that are new in this advisory. The Oracle Database Server, Enterprise Manager, and the Oracle Application Server patches for this Critical Patch Update are cumulative, and contain all the fixes from the previous Critical Patch Update. Risk matrices for these previous fixes can be found in the previous Critical Patch Update advisory.

E-Business Suite patches are not cumulative, so E-Business Suite customers should refer to previous Critical Patch Updates to identify previous fixes they wish to apply.

Oracle Collaboration Suite patches are not cumulative, so Oracle Collaboration Suite customers should refer to previous Critical Patch Updates to identify previous fixes they wish to apply.

One vulnerability appearing in two Risk Matrices

Several vulnerabilities addressed by this Critical Patch Update are in both the Database Server and Application Server products. The Risk Matrices show these shared vulnerabilities by specifying the **Vuln #**s from both matrices on a single vulnerability row.

Risk Matrix Definitions

MetaLink Note 293956.1 defines the terms used in the Risk Matrices.

Risk Analysis and Blended Attacks

Oracle has analyzed each potential vulnerability separately for risk of exploit and impact of exploit. Oracle has performed no analysis on the likelihood and impact of blended attacks (i.e. the exploitation of multiple vulnerabilities combined in a single attack).

Policy Statement on Information Provided in Critical Patch Updates and Security Alerts

Oracle Corporation conducts an analysis of each security vulnerability addressed by a Critical Patch Update (CPU) or a Security Alert. The results of the security analysis are reflected in the associated documentation describing, for example, the type of vulnerability, the conditions required to exploit it and the result of a successful exploit. Oracle provides this 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 will not provide additional information about the specifics of vulnerabilities beyond what is provided in the CPU or Security Alert notification, the pre-installation notes, the readme files, and FAQs. Oracle does not provide advance notification on CPU or Security Alerts to individual customers. Finally, Oracle does not develop or distribute active exploit code nor “proof-of-concept” code for vulnerabilities in our products.

Critical Patch Update Availability for De-Supported Versions

Critical Patch Updates are available for customers who have purchased Extended Maintenance Support (EMS). 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) are entitled to download existing fixes; however, new issues that may arise from the application of patches are not covered under ES. Therefore, ES customers should have comprehensive plans to enable removal of any applied patch.

Oracle will not provide Critical Patch Updates for product versions which are no longer covered under the Extended Maintenance Support plan. We recommend that customers upgrade to the latest supported version of Oracle products in order to obtain Critical Patch Updates.

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

References

- Critical Patch Update – April 2005 FAQ, MetaLink Note 301041.1
- MetaLink Note 293956.1 defines the terms used in the Risk Matrix.
- Oracle Critical Patch Update Program General FAQ, MetaLink Note 290738.1
- Oracle Critical Patch Update Documentation Map, MetaLink Note 304410.1
- Security Alerts and Critical Patch Updates- Frequently Asked Questions, MetaLink Note 237007.1

Credits

The following people discovered and brought security vulnerabilities addressed by this Critical Patch Update to Oracle's attention: Esteban Martínez Fayó of Application Security, Inc., Stephen Kost of Integrigy, David Litchfield of NGSS Limited.

Modification History

12-APR-05: Initial release, version 1

13-APR-05: Corrected link to the Oracle Critical Patch Update Documentation Map

Appendix A

Oracle Database Server Risk Matrix

Critical Patch Update – April 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	***Component***	***Access Required (Protocol)***	***Authorization Needed (Package or Privilege Required)***	***Ease***	***Impact***	***Ease***	***Impact***	***Ease***	***Impact***	***Earliest Supported Release Affected***	**Last Affected Patch set (per Supported Release)**	**Workaround**
DB01	Change Data Capture	SQL (Oracle Net)	Database (execute on DBMS_CDC_IPUBLISH)	Easy	Wide	Easy	Wide	---	---	10*g*	10.1.0.4(10*g*)	---
DB02	Change Data Capture	SQL (Oracle Net)	Database (execute on DBMS_CDC_{I}SUBSCRIBE)	Easy	Wide	Easy	Wide	---	---	9*i*R2	9.2.0.5(9*i*), 10.1.0.4(10*g*)	---
DB03	Data Pump	SQL (Oracle Net)	Database (execute on dbms_metadata)	Easy	Wide	Easy	Wide	---	--	9*i*	9.0.1.5(9*i*), 9.0.4.0(9*i*), 9.2.0.6 (9*i*R2), 10.1.0.4(10*g*)	---
DB04	Intermedia	SQL (Oracle Net)	Database (execute on ordsys)	---	---	---	---	Easy	Wide	9*i*R2	9.2.0.5(9*i*R2), 10.1.0.2(10*g*)	---
DB05	Authentication	SQL (Oracle Net)	None	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*	9.0.1.5(9*i*), 9.0.4.0(9*i*)	---
DB06 AS16	Database SSL Library	Network (HTTPS)	None	---	---	---	---	Difficult	Wide	10*g*	10.1.0.3(10*g*)	---
DB07	Internet Directory	Network (LDAP)	None	Easy	Limited	---	---	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB08	Spatial	SQL (Oracle Net)	Database (execute on mdsys.prvt_idx)	Easy	Wide	Easy	Wide	---	---	9*i*	9.0.1.5(9*i*), 9.2.0.5(9*i*R2), 10.1.0.3(10*g*)	---
DB09	XML Database	Network (HTTPS)	None	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*	9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB10	XDK	SQL (Oracle Net)	Database (execute on SYS_DBURIGEN)	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*	9.0.1.4(9*i*)	---
DB11	HTML DB	Local	OS	Easy	Wide	---	---	---	---	1.3	1.3.6, 1.4.4.00.33	---
DB12 AS03	Oracle HTTP Server	Local / Network (HTTP)	OS	Difficult	Limited	Difficult	Limited	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB13 AS04	Oracle HTTP Server	Network	None	---	---	---	---	Difficult	Limited	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---

DB14 AS05	Oracle HTTP Server	Local	OS	Difficult	Limited	Difficult	Limited	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB15 AS06	Oracle HTTP Server	Network (HTTP)	None	---	---	---	---	Easy	Limited	10*g*	10.1.0.4(10*g*)	---
DB16 AS07	Oracle HTTP Server	Network (HTTP)	None	---	---	---	---	Difficult	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB17 AS08	Oracle HTTP Server	Local	OS	Difficult	Wide	Difficult	Wide	Difficult	Limited	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB18 AS09	Oracle HTTP Server	Network (HTTP)	None	Difficult	Limited	Difficult	Limited	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB19 AS11	Oracle HTTP Server (SSL)	Network (HTTPS)	None	---	---	---	---	Easy	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB20 AS12	Oracle HTTP Server (SSL)	Network (HTTPS)	None	---	---	---	---	Difficult	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB21 AS13	Oracle HTTP Server (SSL)	Local	OS	Difficult	Limited	Difficult	Limited	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB22 AS14	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---
DB23 AS15	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Limited	---	---	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2)	---
DB24 AS17	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Limited	---	---	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5(9*i*), 9.0.4.0 (9*i*), 9.2.0.6(9*i*R2), 10.1.0.4(10*g*)	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Database Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Database Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Database Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle Database Vulnerabilities

There are no recommended workarounds for the Oracle Database vulnerabilities described in the Oracle Database Risk Matrix.

Appendix B

Oracle Application Server Risk Matrix

Critical Patch Update – April 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	*Component*	*Access Required (Protocol)*	*Authorization Needed (Package or Privilege Required)*	*Ease*	*Impact*	*Ease*	*Impact*	*Ease*	*Impact*	*Earliest Supported Release Affected*	*Last Affected Patchset*	Workaround
AS01 APPS05	Forms	Network (HTTP)	Authenticated User	Easy	Wide	Easy	Wide	---	---	8	8.0.6.3(8)	---
AS02	mod_jserv	Network (HTTP)	None	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2	---
AS03 DB12	Oracle HTTP Server	Local / Network (HTTP)	OS	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS04 DB13	Oracle HTTP Server	Network	None	---	---	---	---	Difficult	Limited	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1	---
AS05 DB14	Oracle HTTP Server	Local	OS	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1	---
AS06 DB15	Oracle HTTP Server	Network (HTTP)	None	---	---	---	---	Easy	Limited	9.0.4.0	9.0.4.1	---
AS07 DB16	Oracle HTTP Server	Network (HTTP)	None	---	---	---	---	Difficult	Wide	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS08 DB17	Oracle HTTP Server	Local	OS	Difficult	Wide	Difficult	Wide	Difficult	Limited	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS09 DB18	Oracle HTTP Server	Network (HTTP)	None	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS10	Oracle Help	Network (HTTP)	None	Easy	Wide	---	---	---	---	1.0	1.0.7	---
AS11 DB19	Oracle HTTP Server (SSL)	Network (HTTPS)	None	---	---	---	---	Easy	Wide	1.0.2.2	1.0.2.2	---
AS12 DB20	Oracle HTTP Server (SSL)	Network (HTTPS)	None	---	---	---	---	Difficult	Wide	1.0.2.2	1.0.2.2	---
AS13 DB21	Oracle HTTP Server (SSL)	Local	OS	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1	---

AS14 DB22	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Wide	Difficult	Wide	Easy	Wide	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS15 DB23	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Limited	---	---	---	---	1.0.2.2	1.0.2.2	---
AS16 DB06	Oracle HTTP Server (SSL)	Network (HTTPS)	None	---	---	---	---	Difficult	Wide	1.0.2.2	1.0.2.2	---
AS17 DB24	Oracle HTTP Server (SSL)	Network (HTTPS)	None	Difficult	Limited	---	---	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS18	Wireless	Network (MobileXML or XHTML)	None	---	---	---	---	Easy	Wide	9.0.4.0	9.0.4.1	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Application Server Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Application Server Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Application Server Vulnerabilities

No further conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle Application Server Vulnerabilities

There are no recommended workarounds for the Oracle Application Server vulnerabilities described in the Oracle Application Server Risk Matrix.

Appendix C

Oracle Collaboration Suite Risk Matrix

Critical Patch Update – April 2005

				RISK						
				Confidentiality		Integrity		Availability		
Vuln#	*Component*	*Access Required (Protocol)*	*Authorization Needed (Package or Privilege Required)*	*Ease*	*Impact*	*Ease*	*Impact*	*Ease*	*Impact*	Work-around
OCS01	Email Server	Network (HTTP)	authenticated OCS user	Easy	Wide	---	---	---	---	---
OCS02	Email Server	Network (HTTP)	None	---	---	Easy	Limited	---	---	---
OCS03	Email Server	Network (LDAP)	authenticated OCS user	Easy	Wide	Easy	Wide	---	---	---
OCS04	Email Server	Network (SMTP)	None	Difficult	Limited	---	---	---	---	---
OCS05	Email Server	Network (SMTP)	None	---	---	---	---	Easy	Limited	---
OCS06	Email Server	Network (NNTP)	None	---	---	---	---	Easy	Limited	---
OCS07	Email Server	Network (SMTP)	None	---	---	---	---	Difficult	Limited	---
OCS08	Email Server	Network (HTTP)	authenticated OCS user	---	---	Easy	Limited	---	---	---
OCS09	Email Server	Network (SMTP)	None	Difficult	Wide	Difficult	Wide	Difficult	Wide	---
OCS10	Calendar	Network (HTTP)	authenticated OCS user	Easy	Limited	---	---	---	---	---
OCS11	Calendar	Network (CALENDAR)	None	Easy	Limited	---	---	---	---	---
OCS12 OCS13	Calendar	Local access to client computer	None	Difficult	Limited	---	---	---	---	---
OCS14	Calendar	Network	None	Difficult	Limited	---	---	---	---	---

OCS15	Calendar	Network (CALENDAR)	authenticated OCS user	Difficult	Limited	---	---	---	---	---
OCS16	Calendar	Network (CALENDAR)	authenticated OCS user	Difficult	Limited	---	---	---	---	---
OCS17	Calendar	Network (CALENDAR)	authenticated OCS user	Difficult	Limited	---	---	---	---	---
OCS18	Calendar	Network (CALENDAR)	None	Difficult	Limited	---	---	---	---	---
OCS19	Calendar	Network (CALENDAR)	None	Difficult	Wide	---	---	---	---	---
OCS20	Calendar	Network (CALENDAR)	None	Difficult	Limited	---	---	---	---	---
OCS21	Calendar	Network (CALENDAR)	None	Difficult	Limited	---	---	---	---	---
OCS22	Calendar	Network (CALENDAR)	None	---	---	---	---	Easy	Wide	---
OCS23	Calendar	Network (CALENDAR)	None	Difficult	Wide	---	---	---	---	---
OCS24	Calendar	Network (CALENDAR)	None	---	---	---	---	Easy	Wide	---
OCS25	Calendar	Network (HTTP)	authenticated OCS user	Difficult	Limited	Difficult	Limited	---	---	---
OCS26	Wireless	Network (HTTP)	None	Easy	Limited	---	---	---	---	---
OCS27	Wireless	Network (HTTP)	None	Difficult	Wide	---	---	---	---	---
OCS28	Conferencing	Local access to client computer	None	Easy	Limited	Easy	Limited	---	---	---
OCS29	Conferencing	Network (HTTP)	authenticated OCS user	Easy	Limited	---	---	---	---	---
OCS30	Conferencing	Network (HTTP)	None	Difficult	Limited	Difficult	Limited	---	---	---

OCS31	Conferencing	Network (HTTP)	authenticated OCS user	---	---	Easy	Limited	---	---	---
OCS32	Conferencing	Network (HTTP)	None	Difficult	Wide	Difficult	Wide	---	---	---
OCS33	Conferencing	Network (HTTP)	None	Easy	Limited	---	---	---	---	---
OCS34	Conferencing	Network (HTTP)	None	Easy	Wide	Easy	Wide	Easy	Wide	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Collaboration Suite Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Collaboration Suite Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Collaboration Suite Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle Collaboration Suite Vulnerabilities

There are no recommended workarounds for the Oracle Collaboration Suite vulnerabilities described in the Oracle Collaboration Suite Risk Matrix.

Appendix D

Oracle E-Business Suite Risk Matrix
Critical Patch Update – April 2005

			RISK								
			Confidentiality		Integrity		Availability				
Vuln#	***Access Required (Protocol)***	***Authorization Needed (Package or Privilege Required)***	***Ease***	***Impact***	***Ease***	***Impact***	***Ease***	***Impact***	***Earliest Supported Release Affected***	**Last Affected Patch set**	**Workaround**
APPS01	Network (HTTP)	Authenticated User	Easy	Wide	---	---	---	---	11.5.0	11.5.10	---
APPS02	Network (HTTP)	None	Easy	Limited	---	---	---	---	11.5.8	11.5.10	---
APPS03	Network (HTTP)	None	---	---	---	---	Easy	Limited	11.5.0	11.5.10	---
APPS04	Network (HTTP)	None	Easy	Limited	Easy	Limited	---	---	11.5.0	11.5.10	---
APPS05 AS01	Network (HTTP)	Authenticated User	Easy	Wide	Easy	Wide	---	---	11.0	11.5.8	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle E-Business Suite Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle E-Business Suite Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle E-Business Suite Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities. An installed version of Oracle E-Business Suite and a connected session are sufficient.

Workarounds, Oracle E-Business Suite Vulnerabilities

There are no recommended workarounds for the Oracle E-Business Suite vulnerabilities described in the Oracle E-Business Suite Risk Matrix.

Appendix E

Oracle Enterprise Manager Grid Control Risk Matrix
Critical Patch Update – April 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	*Component*	*Access Required (Protocol)*	*Authorization Needed (Package or Privilege Required)*	*Ease*	*Impact*	*Ease*	*Impact*	*Ease*	*Impact*	*Earliest Supported Release Affected*	Last Affected Patch set	Workaround
EM01	Oracle Management Agent	Network	None	---	---	---	---	Easy	Wide	9.0.4	9.0.4.1, 10.1.0.3	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Enterprise Manager Grid Control Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Enterprise Manager Grid Control Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Enterprise Manager Grid Control Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle Enterprise Manager Grid Control Vulnerabilities

There are no recommended workarounds for the Oracle Enterprise Manager Grid Control vulnerabilities described in the Oracle Enterprise Manager Grid Control Risk Matrix.

Appendix F

Oracle PeopleSoft Applications Risk Matrix

Critical Patch Update – April 2005

				RISK							
				Confidentiality		Integrity		Availability			
Vuln#	*Component*	*Access Required*	*Authorization Needed*	*Ease*	*Impact*	*Ease*	*Impact*	*Ease*	*Impact*	**Products Affected**	*Work-around*
PS01	Role Chooser	Network	Valid EnterpriseOne login	Easy	Limited	Easy	Limited	---	---	EnterpriseOne applications (8.9 SP2 and 8.93)	Enable Role Chooser to avoid unauthorized access
PS02	Row Security	Network	Valid EnterpriseOne login	Easy	Limited	Easy	Limited	---	---	EnterpriseOne web applications(8.9 SP2 and 8.93)	---
PS03	Row Security	Network	Valid EnterpriseOne login	Difficult	Limited	Easy	Limited	---	---	EnterpriseOne applications (8.9 SP2 and 8.93) and OneWorldXe/ERP8 applications (SP22 and higher)	---
PS04	Row Security	Network	Valid EnterpriseOne login	Difficult	Limited	Easy	Limited	---	---	OneWorldXe/ERP8 applications (SP23 and higher)	---
PS05	Row Security	Network	Valid EnterpriseOne login	Difficult	Limited	Easy	Limited	---	---	EnterpriseOne applications (8.9 SP2 and 8.93)	---
PS06	Row Security	Network	Valid EnterpriseOne login	Difficult	Wide	Easy	Wide	---	---	EnterpriseOne web applications (8.9 SP2 and 8.93)	---
PS07	Row Security	Network	Valid EnterpriseOne login	Difficult	Limited	Easy	Limited	---	---	EnterpriseOne web applications (8.9 SP2 and 8.93)	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle PeopleSoft Applications Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, PeopleSoft Applications Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle PeopleSoft Applications Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle PeopleSoft Applications Vulnerabilities

There are no recommended workarounds for the Oracle PeopleSoft Applications vulnerabilities described in the Oracle PeopleSoft Applications Risk Matrix.