Revised: March 2nd, 2005
Severity: 1

Alert #68: Oracle Security Update

Description

This security alert addresses security vulnerabilities in Oracle's server products.

Supported Products Affected

- Oracle Database 10*g* Release 1, version 10.1.0.2
- Oracle9*i* Database Server Release 2, versions 9.2.0.4 and 9.2.0.5
- Oracle9*i* Database Server Release 1, versions 9.0.1.4, 9.0.1.5 and 9.0.1.5 FIPS†
- Oracle8*i* Database Server Release 3, version 8.1.7.4
- Oracle8 Database Release 8.0.6, version 8.0.6.3‡
- Oracle Enterprise Manager Grid Control 10*g*, version 10.1.0.2
- Oracle Enterprise Manager Database Control 10*g*, version 10.1.0.2
- Oracle Application Server 10*g* (9.0.4), versions 9.0.4.0 and 9.0.4.1
- Oracle9*i* Application Server Release 2, versions 9.0.2.3 and 9.0.3.1
- Oracle9*i* Application Server Release 1, version 1.0.2.2

† 9.0.1.5 FIPS was formerly known as Oracle9*i* Database Server Release 1, version 9.0.4.0

‡ Only supported for E-Business Suite customers

The following product releases and versions, and all future releases and versions are **not** affected:

- Oracle Database 10*g* Release 1, version 10.1.0.3
- Oracle Enterprise Manager Grid Control 10*g*, version 10.1.0.3
- Oracle Application Server 10*g* (9.0.4), version 9.0.4.2 (not yet available)

Unsupported products, releases and versions have not been tested for the presence of these vulnerabilities, nor patched, in accordance with section 4.3.3.3 of the Software Error Correction Support Policy (Note 209768.1).

Unsupported Database releases are releases prior to 8.1.7, releases of 8.1.7 on several platforms (for the complete list see Desupport notice 250629.1), patch levels of 9.0.1 prior to 9.0.1.4, and patch levels of 9.2 prior to 9.2.0.4. If you are running one of these releases, you must upgrade to a supported release, and install the latest patch set to get to a supported patch level.

Oracle Database Server Vulnerabilities

The available patches eliminate vulnerabilities in the Database Server and the Listener. The unpatched exposure risk is high; exploiting some of these vulnerabilities requires network access, but no valid user account.

Oracle Database Server Risk Matrix

Please refer to Appendix A - Oracle Database Server Risk Matrix.

Oracle Application Server Vulnerabilities
The available patches eliminate vulnerabilities in the Oracle HTTP Server components of Oracle Application Server. The unpatched exposure risk is high; exploiting these vulnerabilities requires network access, but no valid user account.

Oracle Application Server Risk Matrix
Please refer to Appendix B - Oracle Application Server Risk Matrix.

Oracle Enterprise Manager Vulnerabilities
The available patches eliminate a vulnerability in Oracle Enterprise Manager. The unpatched exposure risk is medium; exploiting this vulnerability requires a valid operating system user account on the Enterprise Manager host.

Oracle Enterprise Manager Risk Matrix
Please refer to Appendix C - Oracle Enterprise Manager Risk Matrix.

Oracle Collaboration Suite Impact
All Collaboration Suite customers should apply the Oracle Database patches to their Information Storage database and the Oracle Application Server-embedded database. Collaboration Suite customers should also apply the application server patch to the Oracle Application Server infrastructure installation and to each Collaboration Suite middle tier installation.

Collaboration Suite customers that have upgraded their Information Storage database to version Oracle Database 10*g* Release 1, version 10.1.0.2 should also apply the Enterprise Manager patch.

E-Business Suite 11*i* Impact
E-Business Suite Release 11*i* customers should apply the available Oracle Database patches to their current Oracle Database Servers, which should be one of the following:

- Oracle8*i* Database Server Release 3, version 8.1.7.4
- Oracle9*i* Database Server Release 2, version 9.2.0.4
- Oracle9*i* Database Server Release 2, version 9.2.0.5

E-Business Suite Release 11i customers should also apply the following patches to every node:

- Oracle 9*i* Application Server Release 1, version 1.0.2.2
  [Note: Apply this patch to the Oracle HTTP Server Oracle home, called "iAS"]
- Oracle8 Database Release 8.0.6, version 8.0.6.3
  [Note: Apply this patch to the Oracle Developer 6i Oracle home, called "8.0.6"]

E-Business Suite Release 11*i* Early Adopter customers implementing MetaLink note 233436.1 "Installing Oracle Application Server 10*g* with Oracle E-Business Suite Release 11*i*" should apply the Oracle Application Server patch to their Oracle Application Server release:

- Oracle Application Server 10*g* (9.0.4.0.0)

Oracle Applications 11.0 Impact

Oracle Applications 11.0 customers should apply the available Oracle Database patches to their current Oracle Database Servers, which should be the following:

- Oracle8*i* Database Server Release 3, version 8.1.7.4

The Oracle Application Server delivered with release 11.0 does not require patching because the affected components did not exist.

How to Minimize Risk

Workarounds for vulnerabilities are discussed in the appropriate appendix. Oracle strongly recommends that customers apply the available patches without delay. Please see

http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf

for a definition of severity ratings.

NOTE: Oracle has received notification that there are published exploits for some of the issues addressed in this alert.

Patch Availability

Please see MetaLink Document ID 281189.1:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1

for the patch download procedures and for the Patch Availability Matrix for this Oracle Security Alert.

Please review MetaLink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable. Oracle strongly recommends that you comprehensively test the stability of your system upon application of any patch prior to deleting any original files that are replaced by the patch.

References

- http://www.securityfocus.com/bid/10871
- http://www.kb.cert.org/vuls/id/316206

General Oracle Security Resources

- Alert 68 FAQ, MetaLink Document ID 282108.1
- Security Alert FAQ, MetaLink Document ID 237007.1
- http://otn.oracle.com/products/ias/pdf/best_practices/security_best_practices.pdf
- http://otn.oracle.com/deploy/security/oracle9ias/
- http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf

- http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
- http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf

Credits

The following people discovered and brought these security vulnerabilities to Oracle's attention: Cesar Cerrudo, Esteban Martínez Fayó, Pete Finnigan, Jonathan Gennick, Alexander Kornbrust of Red Database Security, Stephen Kost of Integrigy, David Litchfield of NGSS Limited, Matt Moore of PenTest Limited, Andy Rees of QinetiQ, Christian Schaller of Siemens CERT.

Modification History

31-AUG-04: Initial release, version 1
24-SEP-04: Updated E-Business Suite information.
27-DEC-04: *Supported Products Affected* and E-Business Suite information updated to include information for patches on Oracle8 Database Release 8.0.6, version 8.0.6.3. This version is supported only for E-Business Suite customers, but has been added for completeness.
02-MAR-05: Added risk matrices

Special Note Regarding Risk Matrices

Several vulnerabilities addressed by Alert 68 are in both the Database and Application Server. The Risk Matrices show these shared vulnerabilities by specifying the **Vuln #**s from both matrices on a single vulnerability row.

Appendix A

Oracle Database Server Risk Matrix

Alert 68

				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*
DB01	Dictionary	SQL(Oracle Net)	Database (untrusted plb file must be run)	Difficult	Wide	Difficult	Wide	Easy	Wide	8	8 (8.0.6.3), 8*i* (8.1.7.4), 9*i* (9.0.1.5),9*i*R2 (9.2.0.5), 9*i*FIPS (9.0.4), 10*g* (10.1.0.2)	---
DB02	Extproc	Network	None	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*	9*i* (9.0.1.5), 9*i*R2 (9.2.0.5), 9*i*FIPS (9.0.4), 10*g* (10.1.0.2)	---
DB03	Core SQL	SQL(Oracle Net)	Database	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8*i* (8.1.7.4), 9*i*FIPS (9.0.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.5)	---
DB04	Oracle Text	SQL(Oracle Net)	Database (execute on ctx_output)	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.5)	---
DB05	DDL	SQL(Oracle Net)	Database (grant on create tablespace)	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB06	Core SQL	SQL(Oracle Net)	Database (execute on sys.dbms_system)	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB07	Core SQL	SQL(Oracle Net)	Database (execute sys_context)	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB08	Core SQL	SQL(Oracle Net)	Database (execute on sys.standard)	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*R2	9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB09	Export	SQL(Oracle Net)	Database execute on dbms_report_extension)	Easy	Wide	Easy	Wide	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB10	Oracle Spatial	SQL(Oracle Net)	Database (insert on mdsys.user_sdo_lrs_metadata)	Difficult	Limited	Difficult	Limited	---	---	9*i*R2	9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB11	Oracle Spatial	SQL(Oracle Net)	Database (insert on mdsys.user_sdo_geom_metadata)	Difficult	Limited	Difficult	Limited	---	---	9*i*R2	9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB12 AS03	Listener	Network	None	---	---	---	---	Difficult	Wide	8	8 (8.0.6.3), 8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB13	XDB	Network	None	---	---	---	---	Easy	Limited	9*i*R2	9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB14	DBCA	Local	OS (read access to logfiles in ORACLE_HOME)	Easy	Wide	---	---	---	---	10*g*	10*g* (10.1.0.2)	---

DB15	Oracle Text	SQL(Oracle Net)	Database (execute on ctxsys)	Easy	Wide	Easy	Wide	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.4), 10*g* (10.1.0.2)	---
DB16	Oracle Spatial	SQL(Oracle Net)	Database (any access to mdsys.sdo_txn_inserts)	Difficult	Limited	Difficult	Limited	---	---	10*g*	10*g* (10.1.0.2)	---
DB17	DDL	SQL(Oracle Net)	Database (grant on create type body)	Difficult	Wide	Difficult	Wide	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB18	JDBC	SQL(Oracle Net)	Database (execute SQL from Java)	Difficult	Wide	Difficult	Wide	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB19	DDL	SQL(Oracle Net)	Database (create nested table)	Difficult	Wide	Difficult	Wide	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB20	Scheduler	SQL(Oracle Net)	Database (grant on create job) and OS	Easy	Wide	Easy	Wide	---	---	10*g*	10*g* (10.1.0.2)	---
DB21 AS04	Listener	Network	None	Difficult	Limited	---	---	---	---	8	8 (8.0.6.3), 8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*FIPS (9.0.4), 9*i*R2 (9.2.0.5)	Yes
DB22 AS02	mod_plsql	Network (HTTP)	Database	Difficult	Limited	Difficult	Limited	---	---	8*i*	8*i* (8.1.7.4), 9*i* (9.0.1.5), 9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB23	Core SQL	SQL(Oracle Net)	Database (grant on alter session)	Difficult	Wide	Difficult	Wide	Easy	Wide	9*i*	9*i* (9.0.1.5), 9*i*R2 (9.2.0.4)	---
DB24	Ultrasearch	SQL(Oracle Net)	Database (execute on wksys.wk_adm)	---	---	Easy	Limited	---	---	10*g*	10*g* (10.1.0.2)	---
DB25	Ultrasearch	SQL(Oracle Net)	Database (execute on wksys.wk_acl)	Difficult	Wide	Difficult	Wide	---	---	9*i*R2	9*i*R2 (9.2.0.5), 10*g* (10.1.0.2)	---
DB26	Ultrasearch	SQL(Oracle Net)	Database (execute on wksys.wk_acl)	Difficult	Wide	---	---	---	---	10*g*	10*g* (10.1.0.2)	---
DB27	SQLPLUS	Network (HTTP)	None	Easy	Limited	---	---	---	---	10*g*	10*g* (10.1.0.2)	---
DB28	SQLPLUS	Network (HTTP)	None	---	---	---	---	Easy	Limited	10*g*	10*g* (10.1.0.2)	---

- 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

These are additional conditions that are required in order to exploit the given vulnerability.

- *DB01* A user must be forced to run an untrusted wrapped procedure file to exploit this vulnerability.
- *DB04* The ability to execute procedures in the *ctx_output* package is necessary.
- *DB05* The ability to *create tablespace* is necessary.
- *DB06* The ability to execute procedures in the *sys.dbms_system* package is necessary.
- *DB07* The ability to execute *sys_context* is necessary.
- *DB08* The ability to execute procedures in the *sys.standard* package is necessary.
- *DB09* The ability to execute procedures in the *dbms_report_extension* package is necessary.
- *DB10* The ability to insert into *mdsys.user_sdo_lrs_metadata* is necessary.
- *DB11* The ability to insert into *mdsys.user_sdo_geom_metadata* is necessary.
- *DB14* The ability to read logfiles in the ORACLE_HOME hierarchy is necessary.
- *DB15* The ability to execute procedures in the *ctxsys* package is necessary.
- *DB17* Access to *mdsys.sdo_txn_inserts* is necessary.
- *DB18* The ability to execute SQL from Java is necessary.
- *DB19* The ability to create a nested table is necessary.
- *DB20* The ability to *create job* is necessary, as well as a valid account on the server on which the database is running.
- *DB23* The ability to *alter session* is necessary.
- *DB24* The ability to execute procedures in the *wksys.wk_adm* package is necessary.
- *DB25* The ability to execute procedures in the *wksys.wk_acl* package is necessary.

Workarounds, Oracle Database Vulnerabilities

- *DB21 / AS04* Ensure that all IP addresses and hostnames in *tcp.invited_nodes* are valid and reachable.

Appendix B

Oracle Application Server Risk Matrix

Alert 68

				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***
AS01	mod_oradav	Network (HTTP)	Valid Session	Difficult	Limited	Difficult	Limited	---	---	9.0.2.3	9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS02 DB22	mod_plsql	Network (HTTP)	Database	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	1.0.2.2, 9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS03 DB12	Listener	Network	None	---	---	---	---	Difficult	Wide	9.0.2.3	9.0.2.3, 9.0.3.1, 9.0.4.1	---
AS04 DB21	Listener	Network	None	Difficult	Limited	---	---	---	---	9.0.2.3	9.0.2.3, 9.0.3.1, 9.0.4.1	Yes

- 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

- *AS04 / DB21* Ensure that all IP addresses and hostnames in *tcp.invited_nodes* are valid and reachable.

Appendix C

Oracle Enterprise Manager Risk Matrix

Alert 68

				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	Configuration	OS	OS (ability to read files under ORACLE_HOME)	Easy	Wide	Easy	Wide	---	---	10*g*	10*g* (10.1.0.2)	---

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

Required Conditions, Oracle Enterprise Manager Vulnerabilities

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

Workarounds, Oracle Enterprise Manager Vulnerabilities

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