Revised: September 24, 2004
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 9.0.4
- Oracle8*i* Database Server Release 3, version 8.1.7.4
- 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

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 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 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 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 11*i* customers should also apply the Oracle Application Server patch to their current Oracle Application Server release, which should be the following:

- Oracle 9*i* Application Server Release 1, version 1.0.2.2

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
There are no workarounds that fully address the security vulnerabilities that are the subject of this alert. 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.