

Oracle Security Alert 63

Dated: 18 February 2004

Severity: 2

Security Vulnerabilities in Oracle9i Lite

Description

Security vulnerabilities have been discovered in Oracle9i Lite.

Supported Products Affected

- Oracle9i Lite, Versions 5.0.0.0.0 to 5.0.2.9.0

Platforms Affected

See Patch Set Availability below.

E-Business 11i Impact

E-Business 11i customers (Mobile Field Service Laptop and Pocket PC using the Oracle9i Lite Mobile Server) must apply the patch set provided in the Patch Set Availability Matrix.

Required Conditions for Exploit

User authentication (i.e., valid login) to Oracle9i Lite Mobile Server is required to exploit these vulnerabilities. A typical default installation of Oracle9i Lite includes the Oracle9i Lite Mobile Server.

Risk to Exposure

Risk to exposure is moderate since the security vulnerabilities are not exploitable by unauthenticated users of Oracle9i Lite Mobile Server. However the potential impact can be high as an authenticated, knowledgeable and malicious user may be able to gain unauthorized access to a connected Oracle database server if the Oracle9i Lite Mobile Server is installed. These vulnerabilities cannot be exploited if only the Oracle9i Lite Mobile Development Kit (MDK) is installed and the Oracle9i Lite Mobile Server is not.

How to Minimize Risk

There is no workaround that fully addresses the security vulnerabilities described in this Alert.

Ramification for Customer

Oracle strongly recommends that customers apply the patch set for these security vulnerabilities. Please refer to the following document for a definition of Oracle's severity ratings:

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

Patch Set Availability

Please see MetaLink Document ID 261992.1:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=261992.1

for the patch set download procedures and for the Patch Availability for this alert.

Please note that there are no plans to release a patch set for Oracle9i Lite Version 5.0.0.0.0 or Oracle9i Lite Version 5.0.1.0.0. Customers running Oracle9i Lite Version 5.0.1.0.0 or earlier must upgrade to Oracle9i Lite Version 5.0.2.0.0 before applying the patch set.

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 set.

Credits

Oracle Corporation thanks Alexander Kornbrust for discovering and promptly bringing these potential security vulnerabilities to Oracle's attention.

Modification History

18-FEB-2004: Initial release, version 1