Oracle Security Alert #33
Dated: 17 April 2002

User Privileges Vulnerability in Oracle9i Database Server

Description
A potential security vulnerability has been discovered in Oracle9i database server. It is possible to create a user defined in the Oracle9i database server with limited privileges who can potentially access privileged data using SQL syntax for outer joins. As such, a knowledgeable and malicious user can gain unauthorized access to data in Oracle9i database server.

None of the Oracle8i (Release 8.1.x), Oracle8 (Release 8.0.x) or Oracle7 database server release is affected by this vulnerability.

Products affected
Oracle9*i* Database, Release 9.0.1.x, only

Platforms affected
All

Workarounds
There are no workarounds to protect against this potential vulnerability.

Patch Information
Oracle has fixed the potential vulnerability identified above in the upcoming Oracle Database server release, Oracle9i, Release 2. Patches with the base bug fix number, 2121935, are being made available only for supported releases of Oracle9i, Releases 9.0.1.x, database server on all supported platforms.

Download currently available patches for your platform from Oracle' s Worldwide Support web site, Metalink, http://metalink.oracle.com. Activate the "Patches" button to get to the patches Web page. Enter the base bug fix number indicated above and activate the "Submit" button.

Please check with Metalink or Oracle Worldwide Support Services periodically for patch availability if the patch for your platform is not yet available.

IMPORTANT NOTE: If any view in the Oracle9i database server was created before application of your patch, re-compile all views including string 'JOIN' (as user SYS) immediately after application of your patch.

Oracle strongly recommends that you comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.