Oracle Security Alert #23
Dated: 29 November 2001

1. Oracle Home Environment Variable Buffer Overflow

Description
When the ORACLE_HOME environment variable contains 750 bytes or more, a buffer overflow occurs. This buffer overflow may potentially be used to overwrite variables on an application/OS memory stack. Since the dbsnmp program runs as SETUID root, it is possible to gain elevated privileges, including administrative access, on the operating system (OS). To exploit this vulnerability, the "oracle" user must belong to the "dba" OS group (OSDBA).

Database Releases affected
8.0.6, 8.1.6, 8.1.7, 9.0.1

Platforms affected
Unix only (including Linux)

Workaround
% chmod -s dbsnmp

Patch Information
Oracle has fixed this potential security vulnerability in the Oracle9i database server and has backported the fix to supported Oracle8i database server Releases 8.0.6, 8.1.6, 8.1.7 and 9.0.1. See the attached matrix, dbsnmp_patch_matrix, on OTN for patch/platform information. The base bug filed for this bug was 1918073.

Download the patch for your platform from Oracle' s Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for the patch availability if the patch for your platform is not yet available.

Credits
Oracle Corporation thanks Juan Manuel Pascual Escriba for promptly bringing this vulnerability to our attention.

2. CHOWN Path Environment Variable Vulnerability
Description
The "dbsnmp" executable executes the CHOWN and CHGRP commands on Unix (and Linux) platforms when it runs without using a statically declared path or without first checking the validity of the PATH environment variable specified by the user. Thus, a local user can potentially gain elevated privileges, including root access, on the host operating system.

Database Releases affected
8.0.5, 8.1.5

Platforms affected
Unix only (including Linux)

Workaround
It is strongly recommended that affected users upgrade to Oracle8i database server Release 8.1.6, or higher.

Alternatively, issue the following command in $ORACLE_HOME/bin
% chmod o-rx dbsnmp

Credits
Oracle Corporation thanks Ismael Briones Vilar for promptly bringing this vulnerability to our attention.

3. Oracle Home Environment Variable Validation Vulnerability

Description
A local user may potentially execute arbitrary code and commands via the "dbsnmp" executable included with the Oracle suite. The "dbsnmp" executable will follow the path of the ORACLE_HOME environment variable if supplied by the user. This oversight in input validation makes it possible for a user to create a custom (malicious) directory and force "dbsnmp" to execute malicious programs and libraries in that directory that may lead to arbitrary or targeted code or command execution.

Database Releases affected
8.1.6, 8.1.7

Platforms affected
Unix only (including Linux)

Patch Information
Oracle has fixed this potential security vulnerability in the Oracle8i database server. See the attached matrix, dbsnmp_patch_matrix, on OTN for patch/platform information. (The base bug filed for this bug was 1918073).

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for the patch availability if the patch for your platform is not yet available.

Credits
Oracle Corporation thanks Sung J. Choe for promptly bringing this vulnerability to our attention.

IMPORTANT NOTE
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.