Oracle Security Alert #30
Dated: 5 March , 2002

SNMP Vulnerability in Oracle Enterprise Manager, Master_Peer Agent

Description
A potential security vulnerability has been discovered in the Oracle Enterprise Manager (EM) SNMP monitoring capability for Oracle Database that may result in a potential Denial of Service (DoS) attack against EM's "master_peer" agent.

EM is comprised primarily of two driver programs, the "Intelligent Agent" that performs core EM functionality and the "master_peer" agent that provides monitoring capability for EM when SNMP is being used.

This potential security vulnerability can manifest only when the SNMP monitoring feature is used in addition to the default functionality provided by EM. The "master_peer" agent of EM, which provides the SNMP monitoring capability, is vulnerable to ill-formed SNMP requests that render it unable to respond to further SNMP requests or send unsolicited SNMP messages.

Note: The "Intelligent Agent" is not affected by this potential security vulnerability. Therefore, EM's core functionality such as job submission, event registration, notifications, etc. is not affected.

Products affected
EM Releases 1.6.5, 2.0, 2.1, 2.2, 9.0.1 running on (or "included with"):

- Oracle7 Database, Release 7.3.x
- Oracle8 Database, Releases 8.0.x
- Oracle8*i* Database, Releases 8.1.x
- Oracle9*i* Database, Release 9.0.1.x

Platforms affected
Windows and all Unix platforms that support SNMP variants except for IBM AIX.

Workarounds
There are no workarounds to protect against the SNMP vulnerability.

Patch Information
Oracle has fixed the potential vulnerability identified above in patch/bug fix number **2224724**. Patches will be available only for supported releases of EM and Oracle Database on all platforms that require a patch.

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 patch/bug fix number indicated above and activate the "Submit" button.

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

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.

Credits
Oracle Corporation thanks CERT of Carnegie Mellon University's Software Engineering Institute for bringing this potential security vulnerability to Oracle's attention.