

## **Vulnerability in the Oracle Enterprise Manager Backup and Recovery mechanism**

### **Versions Affected**

The vulnerabilities are found in Oracle Enterprise Manager releases 2.0.4 and 2.1.0 on all platforms. These versions of Oracle Enterprise Manager were distributed with Oracle 8.1.5 and Oracle 8.1.6. Oracle Enterprise Manager release 2.2, distributed with Oracle 8.1.7, contains the process listing vulnerability.

### **Platforms Affected**

All platforms

### **Description**

Several related security vulnerabilities have been discovered in the Oracle Enterprise Manager backup and recovery mechanism. Using these vulnerabilities, a knowledgeable and malicious attacker can potentially gain a higher level of access to the Oracle database.

When a database backup job starts, a temporary file is created. The temporary file contains authentication information for connecting to the Oracle database as SYSDBA. The temporary file is not deleted upon completion of the backup job.

When a database backup job is submitted to Oracle Enterprise Manager Agent, a TCL script file is created. If the backup job uses recovery catalog or is submitted with overriding credentials, the credentials are exposed in the TCL script file.

During execution of a backup job, credentials associated with the backup job are exposed when a process listing operating system command “ps” is executed on UNIX operating systems.

### **Likelihood of Occurrence**

Anytime a backup job is submitted from Enterprise Manager.

### **Possible Symptoms**

Database credentials are exposed as indicated in the description above.

### **Workaround**

None.

### **Patches**

The generic bugs filed against the Oracle Enterprise Manager are 1375503 and 1374495.

The patch eliminates the creation of temporary files containing SYSDBA authentication information during the backup process. The patch removes the credentials from the TCL script file created when a database backup job is submitted to the OEM Agent. The patch prevents credentials from being exposed during execution of a process listing command on UNIX.

The patch for this vulnerability can be downloaded from the Oracle Worldwide Support Services website at <http://metalink.oracle.com>. Navigate to the patch download screen and select Oracle Enterprise Manager from the pull down menu under products. To view the list of available patches for Oracle Enterprise Manager, navigate to the submit button and hit return. Please reference the patch corresponding to your version of OEM.

Oracle Enterprise Manager Version	Patch
OEM 2.2	EM_2.2_1374495
OEM 2.1	EM_2.1_1375503
OEM 2.0.4	EM_2.0.4_1375503