Oracle Security Alert #44
Dated: 04 October 2002
Severity: 1

Unauthorized Access Vulnerability in the Oracle E-Business Suite, Release 11*i*

Description
A potential security vulnerability has been discovered in Oracle E-Business Suite Release 11*i*. Certain patch levels for Release 11*i* contain a vulnerability that allows a knowledgeable and malicious user to bypass the user authentication check and gain unauthorized access to Release 11*i* without proper authentication.

Products Affected
Certain patch levels of Oracle E-Business Suite 11*i* are affected by this problem. To determine if your installation is affected, locate the `APPS.ZIP` file under the `$JAVA_TOP` directory, unzip the `AolSecurityPrivate.class` file, and scan that file for the `$Header` version number.

On Unix, this can be done with the following commands:

```
% unzip $JAVA_TOP/apps.zip oracle/apps/fnd/security/AolSecurityPrivate.class
% strings oracle/apps/fnd/security/AolSecurityPrivate.class | grep '$Header'
```

Installations with `AolSecurityPrivate.class` version 115.7 through version 115.18 are affected.

Platforms Affected
All

Patch Solution
Oracle has fixed the potential security vulnerability identified above, under ***Mandatory Applications Security Patch*** for bug number **2609399**. If your system is at an affected patch level, you should apply the patch immediately. Your system should already have the necessary prerequisite software.

Even if your system is not currently at an affected patch level, Oracle strongly recommends that you apply this patch and its prerequisite. Doing so will avoid this potential security vulnerability in the future.

Download currently available patches from Oracle Worldwide Support Services web site, Metalink, (http://metalink.oracle.com). Activate the 'Patches' button to get to the patches web page. Enter Patch Number **2609399** as indicated above, select a platform and activate the 'Submit' button.

Oracle strongly recommends that you backup and 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.