Oracle Security Alert #39
Dated: 08 August 2002
Severity: 1

Oracle9i Application Server - Web Cache Administrator Password Not Encrypted

Description
A potential security vulnerability has been discovered in the Oracle Enterprise Manager Web site. The Oracle Enterprise Manager Web site provided with Oracle9i Application Server Release 9.0.2 provides an HTML interface from which the Web cache administration interface in Oracle9iAS can be launched. The Web cache administration interface requires a password that is not encrypted by default. Thus, a knowledgeable and malicious user can gain unauthorized access to the Web cache administrator password.

Products affected
Web Cache technology in Oracle9*i* Application Server 9.0.2.

Platforms affected
Unix and Linux only
(Windows platforms not affected)

Patch Information
No patch is available for this potential security vulnerability. However, Oracle strongly encourages customers to take the following measures to address this issue.

1. Edit the file, $ORACLE_HOME/sysman/emd/targets.xml.

   Replace **ALL** lines that read:
   <Property NAME="authpwd" VALUE="administrator"/>

   with the following:
   <Property NAME="authpwd" VALUE="administrator" ENCRYPTED="FALSE" />

   (Note that “FALSE” is all capital letters.)

2. Restart the Oracle Enterprise Manager web site or execute "emctl reload" at the command prompt.

Note that restarting (or reloading) the OEM web site changes the line in targets.xml to:
<Property NAME="authpwd" VALUE="xxxx" ENCRYPTED="TRUE" />

(targets.xml is a dynamic file containing field values that may change upon reloading or restarting as is the case above.)

The potential security vulnerability is being tracked internally and will be fixed by default in a future release of Oracle9i Application Server. An Oracle Security Alert identifying the release containing the default fix will be made public on Oracle Technology Network.