Oracle Security Alert #41
Dated: 14 August 2002
Severity: 2

Oracle9i Application Server Oracle Java Server Page (OJSP) Demos Vulnerability

Description
Three potential security vulnerabilities have been discovered in Oracle9i Application Server. A knowledgeable and malicious user can gain unauthorized access to Oracle9i Application Server by crafting cross-site script attacks against OJSP demos in Oracle9i Application Server.

Note that the potential security vulnerability listed above affects only the OJSP demos and does not, in any manner, affect or is related to the Java Server Page (JSP) container in Oracle9i Application Server.

The default URLs for the affected OJSP demos are:

http://host:7778/ojspdemos/basic/hellouser/hellouser.jsp
http://host:7778/ojspdemos/basic/simple/welcomeuser.jsp
http://host:7778/ojspdemos/basic/simple/usebean.jsp

A cross-site script attack containing "<script>alert(document.cookie)</script>" as the text entry field on any of the URLs listed above will cause the "JSESSIONID" value to be displayed in a user's browser.

Products affected
Oracle9*i* Application Server Release 9.0.2
Oracle9*i* Application Server Release 1.0.2.2.x
Oracle9*i* Application Server Release 1.0.2.x

Platforms affected
All the Oracle9*i* Application Server supported platforms.
(Solaris, Linux, HP-UX, AIX, Compaq Tru64, WIndowsNT/2000)

Workarounds
Oracle strongly urges customers to apply the following workaround to address the vulnerabilities mentioned above.

Disable the OJSP demos by removing the affected JSP files in the following URLs (default locations provided below):

/ora9ias/j2ee/OC4J_Demos/applications/ojspdemos/ojspdemos-web/basic/simple
/ora9ias/j2ee/OC4J_Demos/applications/ojspdemos/ojspdemos-web/basic/hellouser

Patch Information
Oracle has fixed the potential security vulnerabilities identified above in Oracle9i Application Server Release 9.0.3, to be made available for public release in the fall of 2002.

Credits
Oracle Corporation thanks Matt Moore of Westpoint Limited and Runa of Oracle Corporation for discovering and promptly bringing these potential security vulnerabilities to Oracle's attention.