Solution for Potential Vulnerability in Granting FilePermission to Oracle Java Virtual Machine

Versions Affected
Oracle8i Release 3 (8.1.7)
Oracle Application Server 9iAS Release 1.0.2.0.1

Platforms Affected
All

Description of the Problem
A potential vulnerability in Oracle JVM has been discovered. The Oracle Servlet Engine in the Oracle JVM security policy recommends granting file permissions in a very controlled manner. When this policy is disregarded and FilePermission is granted to <<ALL FILES>> within a web domain, there exists a potential vulnerability of viewing directories and static files outside the web root with the help of .jsp and .sqljsp extensions.

e.g.
call dbms_java.grant_permission('SCOTT', 'SYS:java.io.FilePermission', '<<ALL FILES>>','read');

Thus, it may also be possible to execute .jsp files outside the web root.

Likelihood of Occurrence
In a Netscape browser, a URL containing "the current hierarchy level" (".") and/or "the level above this hierarchy level" ("..")

Solution
To avoid this vulnerability, grant permission to the explicit document root file path only.

e.g.
call dbms_java.grant_permission('SCOTT', 'SYS:java.io.FilePermission', '(actually directory path)','read');