Workaround for Unintended JSP Execution When Using Oracle Apache/JServ

Description

A potential security vulnerability has been discovered in Oracle JSP Releases 1.0.x through 1.0.2 when using Oracle Apache/JServ only. This vulnerability permits the execution of unintended (or incorrect) JSP files because of a bug in Apache/Jserv path translation. As such, if there exists a URL, http://host:port/servlets/a.jsp, Oracle JSP executes "d:\servlets\a.jsp" if such a directory path actually exists. Thus, a URL virtual path, an actual directory path and the Oracle JSP name (when using Oracle Apache/JServ) must match for this potential vulnerability to occur.

Products Affected

Oracle8i, Release 8.1.7
Internet Application Server, iAS, Releases 1.0.0, 1.0.1 and 1.0.2

Platforms Affected

All

Solution

Ensure that the virtual path in a URL is different from the actual directory path when using Oracle Apache/JServ. Also, do not use the <servletzonepath> directory in "ApJServMount <servletzone-path> <servletzone>" to store data or files.

A bug fix will be developed for Oracle Apache/JServ and available in the next release of iAS.

Credits

Oracle Corporation wishes to thank Georgi Guninski for discovering this vulnerability and promptly bringing it to Oracle's attention.