Vulnerability in the Oracle Listener Program

Overview
A security vulnerability in the listener program of the Oracle Enterprise Edition has been discovered. Using this vulnerability, a knowledgeable and malicious attacker can potentially gain a higher level of access to the Oracle owner account and Oracle databases and introduce malicious code into various operating systems.

Description
The commands SET LOG_FILE and SET TRC_FILE allow the log and trace files, respectively, to which the listener program writes, to be modified dynamically while the listener program is running. The listener program can be configured to append and/or overwrite logging and tracing information to any operating system file that can be written by the Oracle owner, such as an alert file or a database file, and thereby corrupt an Oracle database and potentially introduce malicious code into the operating system.

Affected Products and Releases
Oracle listener program releases 7.3.4, 8.0.6 and 8.1.6 on all platforms except OpenVMS.

Patch Information
The generic bug filed against the Oracle listener program is 1361722.

The patch for this exploit allows a database administrator to restrict run-time administration of the Oracle listener program. A new parameter, ADMIN_RESTRICTIONS_listener_name, has been introduced into listener.ora, the control file for the Oracle listener program. Setting ADMIN_RESTRICTIONS_listener_name=ON prevents the vulnerability from being exploited by disabling the run-time modification of parameters in listener.ora. That is, the listener program will refuse to accept SET commands that alter its parameters and attempting to issue a SET command will result in the generation of an error message. Thus, to change any one of the parameters in listener.ora, including ADMIN_RESTRICTIONS_listener_name itself, this file needs to be edited manually and its parameters need to be reloaded manually (e.g., LSNRCTL RELOAD) for the new changes to take effect without explicitly stopping and restarting the listener program. Operating system access to the protected Oracle account owner directories and files is required to edit listener.ora. Note that the Oracle account owner directories and files must be protected in the operating system by setting the access control permissions on them as recommended by Oracle Corporation in its user manuals.

ADMIN_RESTRICTIONS_listener_name=OFF is the default value when the listener program is installed in order to maintain current customer environments and backward compatibility. There is no change in the run-time behavior of the listener program or in syntax of the SET commands in this mode of operation. Oracle Corporation recommends establishing the listener program password in this mode of operation.

Note that the problem described above does not exist on OpenVMS and thus no patches are required for OpenVMS platform.