

Oracle Security Alert #40
Dated: 08 August 2002
Severity: 3

Oracle Net Listener Vulnerabilities

Description

Two potential vulnerabilities have been discovered in Oracle Net Listener for Oracle9i Release 2 (9.2) Database server.

First, a knowledgeable and malicious user can remotely modify Oracle Net Listener's configuration file (listener.ora) to contain a format string. Doing so may crash the Listener control utility (LSNRCTL) the next time it is used to start up the Listener.

Second, an Oracle DBA can supply input containing format strings to Oracle Net Listener control utility (LSNRCTL) that will crash the Listener upon startup.

Products Affected

Oracle9i Release 2 (9.2 - all releases)
Oracle9i Release 1 (9.0 - all releases)
Oracle8i (8.1 - all releases)
Oracle7, Release 7.3.4

Platforms Affected

All

Workaround

In addition to available patches, Oracle strongly urges customers to take the following steps to address the vulnerabilities identified above.

1. Configure listener password to prevent unauthorized users from administering the listener.

Alternatively, set `ADMIN_RESTRICTIONS_listener_name=ON` in listener.ora to completely disable the runtime modification of listener's configuration parameters.

2. Set appropriate Operating System directory and file permissions on the Listener configuration file, listener.ora.

For example:

Unix: `$ chmod 600 $ORACLE_HOME/network/admin/listener.ora`

Windows: File properties > Security > Permissions ...

3. Do not attempt to start an Oracle Net Listener with an invalid name.

Patch Information

Oracle has fixed the potential vulnerabilities identified above under the base bug number **2395416**.

Download currently available patches from Oracle Worldwide Support Services web site, Metalink (<http://metalink.oracle.com>). Activate the 'Patches' button to get to the patches Web page. Enter bug Number **2395416** as indicated above and activate the 'Submit' button.

Please review MetaLink or check with Oracle Worldwide Support Services periodically for patch availability if the patch for your platform is not available. Please check the matrix provided for details on patch availability.

Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Patch Availability Matrix

Platforms	9.2.0.1	9.0.1.3	8.1.7.4
Solaris-32	Available	Available	Available
IBM-32	N/A	N/A	Available
IBM-64	Available	Available	Available
NT	Available	Available	8/12/02
HP-32	N/A	N/A	Available
HP-64	Available	Available	Available
TRU-64	Available	Available	Available
LINUX (RH 6.0)	N/A	Available	Available
LINUX (SUSE 7.1)	Available	Available	N/A
INTEL SOLARIS	N/A	N/A	Planned
DATA GENERAL	N/A	N/A	Planned
UNIXWARE	N/A	N/A	Planned
IBM NUMA-Q	N/A	N/A	Planned
Solaris-64	Available	Available	Available
SGI-IRIX-64	N/A	N/A	Planned
Siemens-64	N/A	N/A	Planned
Novell (v)	N/A	N/A	N/A
OpenVMS (v)	Planned	Available	Planned
OS/390 (v)	Available	N/A	Available
NEC (v)	N/A	N/A	N/A
Fujitsu-DS (v)	N/A	N/A	N/A
Hitachi (v)	N/A	N/A	N/A
IBM VM	N/A	N/A	N/A

N/A: Either a patch will not be created for that platform and version of Oracle (an upgrade to a patched level of Oracle will be required) or there is no such release for Oracle.

Planned: The patchset is not released as yet; the fix will be included by default upon release.

Credits

Oracle Corporation thanks David Litchfield of Next Generation Security Software Limited for discovering and promptly bringing these potential vulnerabilities to Oracle's attention.