Oracle Security Alert 54
Dated: April 25, 2003
Updated: April 30, 2003
Severity: 2

Buffer Overflow in Oracle Net Services for Oracle Database Server

Description

A potential security vulnerability has been discovered in Oracle Net Services for the Oracle Database server. A knowledgeable and malicious user can cause a buffer overflow in an Oracle database link that may result in a Denial of Service (DoS) attack and/or the execution of arbitrary code against the Oracle Database server.

Products Affected

- Oracle9*i* Release 2
- Oracle9*i* Release 1
- Oracle8*i* (8.1.x – all releases)
- Oracle8 (8.0.x – all releases)
- Oracle7 Release 7.3.x

Platforms Affected

See Patch Availability Matrix.

Required conditions for exploit

Database-authenticated user (i.e., valid login required) and the CREATE DATABASE LINK privilege.

Risk to exposure

Risk to exposure is high, as this buffer overflow can lead to the execution of arbitrary code that may compromise the Oracle host server and/or result in a Denial of Service (DoS) attack against the Oracle Database. Unless you connect the Oracle Database directly to the Internet (e.g., no intervening application server or firewall), a remote exploit via the Internet is, in our opinion, unlikely. Note that we strongly recommend that you do not connect your database directly to the Internet. This vulnerability is susceptible to an insider attack originated on the corporate Intranet if the required conditions mentioned above are met.

How to minimize risk

Follow best practices for database,
http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf &
http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf,
and for IT deployments of firewalls, etc.

Ramification for customer

There are no workarounds that can directly address the potential vulnerability identified above.

Oracle strongly recommends that customers review the severity rating for this Alert and patch accordingly. See http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf for a definition of severity ratings.

Patch Information

The patches listed in the Patch Availability Matrix fix the potential security vulnerability identified above. Please note that this fix is included in the Oracle9i Database Release 2, Version 9.2.0.3 patchset.

The patch READMEs contain the patch application instructions/configuration guide.

Fixed by

An interim (one-off patch) for this issue is available for these affected database versions:

- Oracle 9*i* Release 2, version 9.2.0.2 (excluding Windows)
- Oracle 9*i* Release 1, version 9.0.1.4
- Oracle 8*i* Release 3, version 8.1.7.4
- Oracle8 Database, Version 8.0.6.3 (Desupported release; however, patch is available for Extended Maintenance Support customers.)

Currently there are no plans to release a patch for 8.0.5.x, 8.1.5.x, 8.1.6.x, 7.3.x, or other patchsets of the supported releases.

Download this one-off patch from the Oracle Support Services web site, Metalink (http://metalink.oracle.com).

1. Click on the **Patches** button.
2. Click on the "**New** Metalink Patch Search ".
   If you are not on the "Simple Search" screen, click on the "Simple" button to get to the "Simple Search" screen.
3. Refer to the Patch Availability Matrix below to determine the patch number required.
4. In the "Search By" option select "Patch Numbers(s)" from the drop-down menu, and enter the required patch number in the box.
5. Click on the "Go" button.
6. Select the required platform and language.
7. Click on the "Download" button.
8. Recommended: you should also click on the "View README" button for additional information and instructions.

Please review Metalink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable.

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

Special Note: The patches listed below supersede all patches in Oracle Security Alerts 40 and 42 for Oracle Net Services.

Platforms	9.2.0.2	9.0.1.4	8.1.7.4	8.0.6.3
Sun Solaris (32-bit)	2749511	2760944	2784635	2760879
Sun Solaris (64-bit)	2749511	2760944	2784635	N/A
IBM AIX 4.3.3 and 5L (32-bit)	N/A	N/A	2784635	2760879
IBM AIX 4.3.3 (64-bit)	2749511	2760944	2784635	2760879
IBM AIX Based 5L(64-bit)	2749511	N/A	N/A	N/A
MS Windows NT/2000/XP	N/A	ECD: May 2003	2899111	2845564
HP-UX 10.20	N/A	N/A	N/A	ECD; TBD
HP-UX 11.0 (32-bit)	N/A	N/A	2784635	2760879
HP-UX (64-bit)	2749511	2760944	2784635	2760879
HP Tru64	2749511	2760944	2784635	2760879
LINUX	2749511	2760944	2784635	N/A
LINUX 390	2749511	N/A	N/A	N/A
LINUX IA64	ECD: TBD	N/A	N/A	N/A
INTEL SOLARIS	N/A	N/A	ECD: TBD	N/A
DATA GENERAL	N/A	N/A	ECD: TBD	N/A
UNIXWARE	N/A	N/A	2784635	N/A
IBM NUMA-Q	N/A	N/A	2784635	ECD: MAY 2003
SGI-IRIX-64	N/A	N/A	ECD: TBD	N/A
Siemens-64	N/A	N/A	ECD: TBD	N/A
Novell	N/A	N/A	N/A	N/A
OpenVMS	ECD: TBD	2760944	2784635	N/A
IBM OS/390 (MVS)	2749511	2760944	N/A	N/A
NEC	N/A	N/A	N/A	N/A
HP IA64	ECD: TBD	N/A	N/A	N/A
Fujitsu UXP/DS	N/A	N/A	N/A	2760879
Hitachi RISC Unix	N/A	N/A	N/A	2760879

N/A: The patch for the Oracle Database Release/Version is not available for this platform.

ECD: Expected Completion Date.

Credits

Oracle Corporation thanks David Litchfield, of Next Generation Security Software Ltd., for discovering and promptly bringing this potential security vulnerability to

Oracle's attention. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/research/advisories.html.

Modification History
25-APR-03: Initial release, version 1
30-Apr-03: Updated the patch availability information