

Oracle Security Alert #48
Dated: 11 February 2003
Updated: 03 March 2003
Severity: 1

Buffer Overflow in Oracle Database Server

Description

A potential security vulnerability has been discovered in Oracle Database Server. A knowledgeable and malicious user who has authenticated to the database server can exploit this vulnerability in the form of a buffer overflow against Oracle Database Server.

Products Affected

- Oracle9i Database Release 2, Version 9.2.x
- Oracle9i Database Release 1, Version 9.0.x
- Oracle8i Database, Version 8.1.x
- Oracle8 Database, Version 8.0.x

Oracle7, Version 7.x and earlier versions are **not** affected.

Platforms Affected

See Patch Availability Matrix.

Required conditions for exploit

Database authenticated user (i.e., valid login required).

Risk to exposure

Risk to exposure is high, as buffer overflows can lead to serious problems such as denial of service and session capture. Unless you connect the database directly to the Internet (e.g., no intervening application server or firewall), a remote buffer overflow attack via the Internet is, in our opinion, unlikely. This vulnerability is susceptible to an insider attack originated on the corporate Intranet. Note that we strongly recommend that you do not connect your database directly to the Internet.

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

The patches for Security Alerts 48 through 52 do not conflict with each other; technically, the order in which the patches are applied has no significance, but Oracle recommends applying the patch listed in Alert #51 with the highest priority. See http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf for a definition of severity ratings.

Patch Information

The fix for this potential security vulnerability is **only** available for the latest patchset level (as listed in the **Fixed by** section) for each supported database release on the platforms listed in the Patch Availability Matrix. **If you are not on the latest patchset release, you need to apply the latest patchset before applying this one-off patch.** Please note this fix will be included by default in the Oracle9i Database Release 2, Version 9.2.0.3 patchset.

Fixed by

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

- Oracle 9i Database Release 2 version 9.2.0.2
- Oracle 9i Database Release 1 version 9.0.1.4
- Oracle 8i Database, Version 8.1.7.4
- Oracle8 Database, Version 8.0.6 (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.

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 Search" button.
3. Input the bug number **2642117** on the "Search by Patch Number" box.
4. Click **Go**.
5. Select the patch for the appropriate product version.
6. Select the appropriate platform.
7. Click **Download**.

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 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 for Security Alerts 48 through 52 do not conflict with each other; the order in which the patches are applied has no significance. The patch matrix for Oracle8 Database, Version 8.0.6, will be made available in the next update to this Alert.

| Platforms | 9.2.0.2 | 9.0.1.4 | 8.1.7.4 |
|-------------------------------|------------|------------|------------|
| Sun Solaris (32-bit) | Available | Available | Available |
| Sun Solaris (64-bit) | Available | Available | Available |
| IBM AIX 4.3.3 and 5L (32-bit) | N/A | N/A | Available* |
| IBM AIX 4.3.3 (64-bit) | Available | Available | Available |
| IBM AIX Based 5L(64-bit) | Available | N/A | N/A |
| MS Windows NT/2000/XP | Available+ | Available+ | Planned+ |
| HP-UX (32-bit) | N/A | N/A | Available |
| HP-UX (64-bit) | Available | Available | Available |
| HP Tru64 | Available | Available | Available |
| LINUX | Available | Available | Available |
| LINUX 390 | Planned | N/A | N/A |
| INTEL SOLARIS | N/A | N/A | Available |
| DATA GENERAL | N/A | N/A | Available |
| UNIXWARE | N/A | N/A | Available |
| IBM NUMA-Q | N/A | N/A | Available |
| SGI-IRIX-64 | N/A | N/A | Available |
| Siemens-64 | N/A | N/A | Planned |
| Novell | N/A | N/A | N/A |
| OpenVMS | Planned | Planned | Available |
| IBM OS/390 (MVS) | Available | Available | Available |
| NEC | N/A | N/A | N/A |
| HP IA64 | Planned | N/A | N/A |

***:** For 8.1.7.4 on IBM AIX 5L (32-bit), download the same patch as IBM AIX 4.3.3 (32-bit).

+: The fix for 9.2.0.2 is in 9.2.0.2.1 Patch 1. To obtain this fix download the patch for <[BUG:2814865](#)>.

+: The fix for 9.0.1.4 is in 9.0.1.4.0 Patch 1. To obtain this fix download the patch for <[BUG:2781666](#)>.

+: The fix for 8.1.7.4 will be included in 8.1.7.4 Patch 8.

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

Planned: The patch is not released as yet. Future releases (e.g., 9.2.0.3 and higher) of the Oracle Database Server will contain the fix

by default.

Credits

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

Modification History

21-Feb-2003: The Products Affected and Patch Information sections clarified.

24-Feb-2003: The title was updated. Products Affected and Patch Information sections clarified.

26-Feb-2003: Required conditions, risk to exposure, how to minimize risk, and ramification for customer sections added.

03-Mar-2003: Title updates, minor updates to flow of text and Patch Availability Matrix.