

Oracle Security Alert #46**Dated: 31 October 2002 (updated 11 November 2002)****Severity: 2****Buffer Overflow in iSQL*Plus (Oracle9i Database Server)****Description**

A potential security vulnerability has been discovered in iSQL*Plus, in Oracle9i Database. A knowledgeable and malicious user can pass a USERID parameter that may result in a remote buffer overflow exploit against iSQL*Plus.

This potential security vulnerability does not affect SQL*Plus.

Products affected

Oracle9i Database, Release 1, Release 9.0.x (all releases)

Oracle9i Database, Release 2, Releases 9.2.0.1 and 9.2.0.2

Platforms affected

All

Workarounds

There is no workaround to address the potential security vulnerability identified above.

Patch information

Oracle has fixed the potential security vulnerability identified above under the base bug number **2581911**. Future releases of the Oracle Database server will contain the fix by default.

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 **2581911** 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 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 matrix

| Operating System | 9.0.x | 9.2.0.1 | 9.2.0.2 |
|------------------------------------|-----------|-----------|-------------|
| MS Windows NT/2000/XP Server (912) | Available | Available | 11-Nov-2002 |
| Sun Solaris OS (SPARC) (453) | NR | Available | Available |
| Sun Solaris OS (SPARC) 64-bit (23) | NR | Available | Available |
| Linux Intel (46) | NR | Available | Available |
| Linux for S/390 (211) | NR | Available | 11-Nov-2002 |
| Linux Intel (64-bit) (110) | NR | NR | 11-Dec-2002 |
| HP IA64 HPUnix (197) | NR | NR | 11-Dec-2002 |
| HP (Compaq) Tru-64 Unix (87) | NR | Available | Available |
| HP 9000 Series HP-UX (64-bit) (59) | NR | Available | Available |

| | | | |
|---|----|-----------|-----------|
| IBM RS/6000 AIX 64-bit (38) | NR | Available | Available |
| IBM AIX Based Systems (64-bit) 5L (212) | NR | Available | Available |

NR = Not Released. /SQL*Plus is not available on this platform in this release.

Credits

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