Oracle Net8 Denial of Service Vulnerabilities

1. Offset_to_data value too large
Overview
A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).

When connecting to an Oracle database, a connection is first made to the listener process. This initial packet contains command data, such as the instance to connect to and the client information. This packet also contains a header with a field indicating the offset to the Oracle command data. If this offset is set to an arbitrarily large value that the listener does not expect, then the listener will crash.

Products
Oracle 7.3.x, Oracle8i database server (all releases)

Platforms
Unix only

Patch Solution
Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 (patchsets 8.1.7.2 and 8.1.7.3) and 8.1.6 on all platforms.

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for the patch availability if the patch for your platform is not yet available.

Please see the matrix posted below this Alert for patch availability and schedules.

2. Requester_version value incorrect
Overview
A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).

When connecting to an Oracle database, a connection is first made to the listener process. This initial packet contains command data, such as the instance to connect to and the client information. This packet also contains a header with a field indicating the version of the client drivers and the offset to the Oracle command data. If the version of the driver does not match to the appropriate offset to the command data, the listener will crash.

Products
Oracle 8.0.x, Oracle8i database server (all releases)

Platforms
All platforms

Patch Solution
Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 (patchsets 81.7.2 and 8.1.7.3) and 8.1.6 and Oracle8 Release 8.0.6 on all platforms.

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for patch availability if the patch for your platform is not yet available.

Please see the matrix posted below this Alert for patch availability and schedules.

3. Maximum Transport Data Size too small

Overview

A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).

When connecting to an Oracle database, a connection is first made to the listener process. This initial packet contains command data, such as the instance to connect to and the client information. This packet also contains a header with a field indicating the maximum transport data size of the client's network. If the maximum transport data size is set to 0, the listener will crash.

Products

Oracle8i database server (all releases)

Platforms

Sun Solaris 2.x

Patch Solution

To the best of its capabilities, Oracle has been unable to reproduce this vulnerability. If you believe that you have successfully reproduced this vulnerability, please contact Oracle Security Alerts at secalert_us@oracle.com with full details of the exploit including operating environment, exploit script(s), server trace files and/or other proofs of exploit.

4. Fragmentation Attack

Overview

A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).

In addition to TCP/IP fragmentation, Oracle allows commands to be fragmented at the application layer. This fragmentation allows commands to be sent in two or more different packets. If the first packet of a fragmented command is repeatedly sent and not followed up with the remainder of the command, the listener hangs waiting for the completion of these commands.

Products

All releases of the Oracle Listener (Oracle 7.3.x, Oracle 8.0.x, Oracle 8.1.x)

Platforms

All platforms

Patch Solution

Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 (patchsets 8.1.7.2 and 8.1.7.3) and 8.1.6 and Oracle8 Release 8.0.6 on all platforms.

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for patch availability if the patch for your platform is not yet available.

Please see the matrix posted below this Alert for patch availability and schedules.

Credits

Oracle would like to thank Internet Security Systems (ISS) for discovering these potential security vulnerabilities and promptly bringing them to Oracle's attention.