

Oracle Security Alert #38
Dated: 08 August 2002
Severity: 1

Security vulnerability in Oracle Net (Oracle9i Release 2 Database Server)

Description

A potential security vulnerability has been discovered in Oracle Net Services for Oracle9i Release 2 (9.2) Database that may result in a denial of service (DoS) attack against the Oracle Net Services Listener. A knowledgeable and malicious user can send an invalid command request to the configured listening endpoint of the Listener. This may cause the Listener to crash or otherwise become unavailable. The Listener must be manually restarted in order to regain normal functionality.

Products Affected

Oracle9i Release 2 (9.2 - all releases)
Oracle9i (9.0.x - all releases)

Platforms Affected

All

Workaround

There are no workarounds that can directly address the potential vulnerability identified above. However, Oracle Net Services feature 'Valid Node Checking' can be used to mitigate the risk of this potential security vulnerability before a patch is applied. Valid Node Checking is used to allow or deny access to Oracle server processes from network clients based on IP addresses.

Set the following parameters in `$ORACLE_HOME/NETWORK/ADMIN/SQLNET.ORA` on the database server to enable the valid node checking feature:

```
tcp.validnode_checking = YES  
tcp.invited_nodes = (list of IP addresses)  
tcp.excluded_nodes = (list of IP addresses)
```

For example:

```
tcp.validnode_checking = YES  
tcp.invited_nodes = (192.168.255.1)  
tcp.excluded_nodes = (192.168.255.2, 192.168.255.3)
```

The first parameter turns on the valid node checking feature. The latter two parameters respectively specify the IP addresses that are permitted to make network connections or are denied from making network connections to the Oracle Server processes, including the Oracle Net Services Listener.

Patch Information

Oracle has fixed the potential security vulnerability identified above, under the base bug number **2467947**. 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 **2467947** 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. Please check the matrix provided below for status and 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	9.2.0.2	9.2.0.1	9.0.1.4	9.0.1.3	9.0.1.2
Solaris-32	Planned	Available	Planned	Available	N/A
IBM-64	Planned	Available	Planned	Available	N/A
NT	Planned	Planned	Planned	Planned	N/A
HP-64	Planned	Available	Planned	Available	N/A
TRU-64	Planned	Available	Planned	Available	N/A
Linux	Planned	Available	Planned	Available	N/A
Solaris-64	Planned	Available	Planned	Available	N/A
OpenVMS (v)	Planned	Planned	Planned	Available	N/A
OS/390 (v)	Planned	Available	Planned	N/A	Available

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 of Oracle.

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

* NT/9.2.0.1 - The patch is included in 9.2.0.1 Patch 1.

** NT/9.0.1.3 - The patch is included in the 9.0.1.3 Patch #6 release.

Note: 9.2.0.2 and 9.0.1.4 are the upcoming patchset releases for Oracle9i Release 2 and Oracle9i Release 1 respectively.

Note: For 9.2.0.2 and 9.0.1.4, the patch will be contained within the release themselves. For 9.2.0.1, 9.0.1.3, and 9.0.1.2, the patch is to be applied on top of these existing patchset releases.

Credits

Oracle Corporation thanks X-Force of Internet Security Systems for discovering and promptly bringing this potential security vulnerability to Oracle's attention.