Oracle Redirect Denial of Service Vulnerability

Overview
A potential security vulnerability has been identified in redirected Net8 connections to the Oracle database server. This vulnerability allows an unauthenticated user to consume all the operating system memory on an Oracle server, remote users to deny access to all other users and cause the operating system to crash: Access to the server is denied and a reboot of the server is required.

Products
All Oracle releases (Oracle 7.3.4, Oracle 8.0.x, Oracle 8.1.x)

Platforms
Windows NT

Solution
There is an immediate workaround for this potential security vulnerability. Oracle Net8 (formerly Oracle SQL*Net) has a feature called “valid node checking” which can be used to allow or deny access to Oracle server processes from network clients with specified IP addresses.

The following parameters can be established in PROTOCOL.ORA, a configuration file of Oracle Net8 to implement the valid node checking feature:

```
tcp.validnode_checking = YES
tcp.invited_nodes = {list of IP addresses}
tcp.excluded_nodes = {list of IP addresses}
```

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 denied from making network connections to the Oracle server processes.

A combination of the parameters listed above can effectively prevent the Oracle database server from consuming Windows NT memory in the manner described.

Credits
Oracle would like to thank Internet Security Systems (ISS) for discovering this potential security vulnerability and promptly bringing it to Oracle’s attention.