

Oracle TNS Listener DoS and/or remote memory inspection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-10/msg00258.html>

- *From:* "NGSSoftware Insight Security Research" <nisr@xxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 17 Oct 2007 12:47:44 +0100
-

NGSSoftware Insight Security Research Advisory

Name: Oracle TNS Listener DoS and/or remote memory inspection
Systems Affected: Oracle 8.1.7.4, 10g Release 2 and 1, Oracle 9
Severity: High
Vendor URL: <http://www.oracle.com/>
Author: David Litchfield [davidl@xxxxxxxxxxxxxxxxxx]
Reported: 22nd June 2006
Date of Public Advisory: 17th October 2007
Advisory number: #NISR17102007C

Description

The TNS Listener can be crashed by an attacker causing a Denial of Service; alternatively the attacker can use the same flaw to expose memory contents remotely. This may reveal sensitive information.

Details

There is a bug in GIOP service that can allow an attacker to crash the TNS Listener and/or dump memory. A DWORD in the connect GIOP packet is trusted as the size of the data in the packet. By setting this to a large value (e.g. 0x1FFFF) causes the listener to allocate this much memory then attempt to copy this much data to it – which eventually leads to a read access violation because the source data is less than this number and the process lands in uninitialized memory. If the attacker uses a smaller number, e.g. 0xFFFF they can dump this many bytes from memory. This may reveal sensitive information such as the TNS Listener password.

Fix Information

Oracle was alerted to this flaw on the 22nd of June 2006. A patch has now been made available:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>

Oracle TNS Listener DoS and/or remote memory inspection

NGSSquirrel for Oracle, an advanced vulnerability assessment scanner designed specifically for Oracle, can be used to accurately determine whether your servers is vulnerable to this flaw. More information about NGSSquirrel for Oracle can be found here:

<http://www.ngssoftware.com/products/database-security/ngs-squirrel-oracle.php>

About NGSSoftware

NGSSoftware develops vulnerability assessment and compliancy tools for database servers including Oracle, Microsoft SQL Server, DB2, Sybase and Informix. Headquartered in the United Kingdom NGS has offices in London, St. Andrews (UK), Brisbane, and Perth (Australia) and seattle in the United States; NGSConsulting provide services to some of the largest and most demanding organizations around the globe.

<http://www.ngssoftware.com/>

Telephone +44 208 401 0070

Fax +44 208 401 0076

enquiries@xxxxxxxxxxxxxxxx

—

E-MAIL DISCLAIMER

The information contained in this email and any subsequent correspondence is private, is solely for the intended recipient(s) and may contain confidential or privileged information. For those other than the intended recipient(s), any disclosure, copying, distribution, or any other action taken, or omitted to be taken, in reliance on such information is prohibited and may be unlawful. If you are not the intended recipient and have received this message in error, please inform the sender and delete this mail and any attachments.

The views expressed in this email do not necessarily reflect NGS policy. NGS accepts no liability or responsibility for any onward transmission or use of emails and attachments having left the NGS domain.

NGS and NGSSoftware are trading names of Next Generation Security Software Ltd. Registered office address: 52 Throwley Way, Sutton, SM1 4BF with Company Number 04225835 and VAT Number 783096402