

[NEWS] Oracle TNS Listener DoS and Remote Memory Inspection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00033.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 21 Oct 2007 17:07:04 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Oracle TNS Listener DoS and Remote Memory Inspection

SUMMARY

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. 0 1FFFF) 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.

[NEWS] Oracle TNS Listener DoS and Remote Memory Inspection

Vendor Status:

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

ADDITIONAL INFORMATION

The information has been provided by <<mailto:davidl@xxxxxxxxxxxxxxxx>>
David Litchfield.

The original article can be found at:

<<http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-tns-listener/>>
<http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-tns-listener/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.