

[NEWS] Oracle TNS Listener Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0049.html>

From: support@securiteam.com

Date: 06/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 13 Jun 2002 07:41:55 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Oracle TNS Listener Buffer Overflow

SUMMARY

The Oracle Net Listener contains a remotely exploitable buffer overrun vulnerability that can allow an attacker to gain complete control of a machine running the Oracle 9i Database.

DETAILS

Vulnerable systems:

- * Oracle 9i

The Listener 'listens' on TCP port 1521 for client request to use the database. On receiving a request the client is passed off to an instance of the database. The request, packaged in a valid TNS packet is of the form

```
(DESCRIPTION=(ADDRESS=
(PROTOCOL=TCP)(HOST=x.x.x.x)
(PORT=1521))(CONNECT_DATA=
(SERVICE_NAME=myorcl.ngssoftware.com)
(CID=
(PROGRAM=X:\\ORACLE\\iSuites\\BIN\\SQLPLUSW.EXE)
(HOST=foo)(USER=bar))))
```

Securiteam: [NEWS] Oracle TNS Listener Buffer Overflow

By supplying an overly long SERVICE_NAME parameter, when forming an error message to be written to the log file, a saved return address on the stack is overwritten thus gaining control over the processes execution. Any code supplied by the attacker will run, by default, in the context of the Local SYSTEM account on Windows platforms and as such is a high risk vulnerability. Because the overflow occurs before the error message is actually written to the log file it may be difficult to detect if an attack has occurred. Customers are advised to patch this as soon as is possible.

Fix Information:

NGSSoftware alerted Oracle to this problem on the 13th of May and Oracle have now released patches which are available from the Metalink site. The patch number is 2367681.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nisr@ngssoftware.com>
NGSSoftware Insight Security Research.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Oracle Reports Server Buffer Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)