

[VulnWatch] Oracle TO_TIMESTAMP_TZ Remote System Buffer Overrun (#NISR16022003b)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-02/0023.html>

From: NGSSoftware Insight Security Research (nisr@nextgenss.com)

Date: 02/17/03

From: "NGSSoftware Insight Security Research" <nisr@nextgenss.com>

To: <bugtraq@securityfocus.com>, <vulnwatch@vulnwatch.org>, <ntbugtraq@listserv.ntbugtraq.com>

Date: Mon, 17 Feb 2003 14:12:46 -0800

NGSSoftware Insight Security Research Advisory

Name: Oracle TO_TIMESTAMP_TZ Remote System Buffer Overrun

Systems Affected: All platforms; Oracle9i Database Release 2, 9i Release 1, 8i, 8.1.7, 8.0.6

Severity: High Risk

Category: Remote System Buffer Overrun

Vendor URL: <http://www.oracle.com>

Author: Mark Litchfield (mark@ngssoftware.com)

Date: 16th February 2003

Advisory number: #NISR16022003b

Description

Oracle's database server contains functions for use within queries. The TO_TIMESTAMP_TZ function exists to convert a string into a timestamp with a time zone datatype. This function contains an exploitable buffer overflow vulnerability.

Details

There is a remotely exploitable buffer overflow vulnerability in the TO_TIMESTAMP_TZ function. A normal statement would look like the following, converting a character string to a value of timestamp with time zone:

```
SELECT TO_TIMESTAMP_TZ('2003-02-016 12:00:00 -8:00','YYYY-MM-DD HH:MI:SS  
TZH:TZM') FROM DUAL;
```

By supplying a long character string for the second parameter an attacker can overwrite a saved return address on the stack of Oracle process. Before this issue can be exploited an attacker must be able to log on to the database server with a valid user ID and password, but as the TO_TIMESTAMP_TZ() function can be executed by PUBLIC by default any user of the system can gain control. Any arbitrary code supplied by an attacker would execute with the same privileges as the user running the service; this

VulnWatch: [VulnWatch] Oracle TO_TIMESTAMP_TZ Remote System Buffer Overrun (#NISR16022003b)

account is typically "Oracle" on linux/unix based platforms and Local System on Windows based operating systems such as NT/2000/XP. As such this allows for a complete compromise of the data stored in the database and possibly a complete compromise of the operating system.

Fix Information

NGSSoftware alerted Oracle to this vulnerability on 30th September 2002 and Oracle has produced a patch which is available from

<http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf>

A check for these issues has been added to NGSSquirrel for Oracle, a comprehensive automated vulnerability assessment tool for Oracle Database Servers of which more information is available from the NGSSite

<http://www.ngssoftware.com/software/squirrelfororacle.html>

Further Information

For further information about the scope and effects of buffer overflows, please see

<http://www.ngssoftware.com/papers/non-stack-bo-windows.pdf>

<http://www.ngssoftware.com/papers/ntbufferoverflow.html>

<http://www.ngssoftware.com/papers/bufferoverflowpaper.rtf>

<http://www.ngssoftware.com/papers/unicodebo.pdf>

About NGSSoftware

NGSSoftware design, research and develop intelligent, advanced application security assessment scanners. Based in the United Kingdom, NGSSoftware have offices in the South of London and the East Coast of Scotland. NGSSoftware's sister company NGSConsulting, offers best of breed security consulting services, specialising in application, host and network security assessments.

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

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

Telephone +44 208 401 0070

Fax +44 208 401 0076

enquiries@ngssoftware.com