

# Oracle unauthenticated remote system compromise (#NISR16022003a)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-02/0030.html>

---

**From:** NGSSoftware Insight Security Research ([nisr@NEXTGENSS.COM](mailto:nisr@NEXTGENSS.COM))

**Date:** 02/17/03

Date: Mon, 17 Feb 2003 14:09:56 -0800  
From: NGSSoftware Insight Security Research <[nisr@NEXTGENSS.COM](mailto:nisr@NEXTGENSS.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

NGSSoftware Insight Security Research Advisory

Name: Oracle unauthenticated remote system compromise  
Systems Affected: All platforms; Oracle9i Database Release 2, 9i Release 1, 8i, 8.1.7, 8.0.6  
Severity: Critical Risk  
Category: Remote System Buffer Overrun  
Vendor URL: <http://www.oracle.com>  
Author: Mark Litchfield ([mark@ngssoftware.com](mailto:mark@ngssoftware.com))  
Date: 16th February 2003  
Advisory number: #NISR16022003a

## Description

\*\*\*\*\*

Oracle is the leader in the database market with a 54% market share lead under ERP (Enterprise Resource Planning). The database server is vulnerable to a remotely exploitable buffer overflow vulnerability. What exacerbates this problem is that no valid User ID or password is required by an attacker.

## Details

\*\*\*\*\*

There is a remotely exploitable buffer overflow vulnerability in the authentication process with the Oracle Database Server. By supplying an overly long username when attempting to log onto the database server an attacker can overflow a stack based buffer overwriting the saved return address. Any arbitrary code supplied by an attacker would execute with the same privileges as the user running the service; this 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. As most client applications for Oracle will truncate the length of the username that can be supplied to the database an attacker would need to write their own Oracle "Authenticator" to exploit this issue. That said, NGSSoftware has found one client application that

## NT-Bugtraq: Oracle unauthenticated remote system compromise (#NISR16022003a)

will allow longer usernames so to test if you are vulnerable to this issue, use the LOADPSP utility usually found in "bin" directory found under the OracleHomeInstallDirectory. On Windows, for example, run:

```
C:\ora9ias\BIN>loadpsp -name -user LONGUSERNAME/tiger@iasdb myfile
```

### Fix Information

\*\*\*\*\*

NGSSoftware alerted Oracle to this vulnerability on 30th September 2002. Oracle has reviewed the code and created a patch which is available from:

<http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf>

NGSSoftware advise Oracle database customers to review and install the patch as a matter of urgency.

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>

It is further recommend that Oracle DBAs have their network/firewall administrators ensure that the database server is protected from Internet sourced traffic.

### 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](mailto:enquiries@ngssoftware.com)

oo

Delivery co-sponsored by TruSecure Corporation

oo

TICSA – Anniversary Special – Limited Time

Become TICSA certified for just \$221.25 US when you register before 3/31/03 with PROMO "TS0103" at [www.2test.com](http://www.2test.com). NO membership fees, certification good for 2 years. Price for international delivery just \$296.25 US, with this offer. Offer cannot be combined with any other special and expires 3/31/03. Visit [www.trusecure.com/ticsa](http://www.trusecure.com/ticsa) for full details.

oo