

[NEWS] Multiple Vulnerabilities in Oracle Database (Character Conversion, Extproc, Password Disclosure, ISQLPlus, TNS Listener)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0095.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 11:06:04 +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>

Multiple Vulnerabilities in Oracle Database (Character Conversion,
Extproc, Password Disclosure, ISQLPlus, TNS Listener)

SUMMARY

Multiple vulnerabilities were discovered in the (Oracle database server Character Conversion, Extproc, Password Disclosure, ISQLPlus, TNS Listener). All the vulnerabilities are addressed in a new cumulative patched issued by Oracle.

DETAILS

Vulnerable Systems:

* Oracle 10g on all operating systems

1. Character Conversion Bugs

Due to character conversion problems in Oracle 10g with Oracle's Application server it is possible to bypass pl/sql exclusions and gain access to the database server as SYS. There is a character conversion bug in 10g that can lead to a compromised backend database server. Both Windows and Linux are affected. Consider the following set up. There's a Oracle HTTP Server (running apache 1.3.22 on Windows) using the PL/SQL

eam: [NEWS] Multiple Vulnerabilities in Oracle Database (Character Conversion, Extproc, Password Disclosure, ISQLPlus

module feeding into a 10g box running on Windows and a 10g box running on Linux. The character set for both instances is WE8ISO8859P1.

When the app server receives a request of:

<http://server/pls/windad/%FF%FF%FF%FF%FF>

The %FFs are converted to the byte 0xFF (as expected) but sniffing the database response to the app server we get:

"ORA-06550: line 8, column 2: PLS-00201: identifier 'YYYYY' must be declared....."

In Oracle 10g, when using the WE8ISO8859P1 character set, converts 0xFF to 0x59 – that is uppercase Y. Due to this conversion an attacker can perform the following request:

http://server/pls/windad/S%FFS.OWA_UTIL.CELLSPRINT?P_THEQUERY=select+username+from+all_users

And therefore gain access to "banned" and dangerous procedures. The character set for the HTTP server is set to: AMERICAN_AMERICA.WE8ISO8859P1.

If, however, we set the character set on the HTTP Server to ENGLISH_UNITEDKINGDOM.WE8MSWIN1252 not only is the 0xFF still converted to 0x59 but if the following is requested:

<http://server/pls/windad/%9F%9F%9F%9F%9F%9F>

The _app_server_ (note – not 10g) converts the %9F to a Y and again this allows us to do the following:

http://server/pls/windad/S%9FS.OWA_UTIL.CELLSPRINT?P_THEQUERY=select+username+from+all_users

And again giving access to the "banned" and dangerous procedures. Other character sets and scenarios may cause similar problems.

2. Extproc Buffer Overflow (long lib name)

The Oracle database server supports PL/SQL, a programming language. PL/SQL can execute external procedures via extproc. Over the past few years there has been a number of vulnerabilities in this area (

<<http://www.nextgenss.com/advisories/oraplsxtproc.txt>>

<http://www.nextgenss.com/advisories/oraplsxtproc.txt>,

<<http://www.nextgenss.com/advisories/ora-extproc.txt>>

<http://www.nextgenss.com/advisories/ora-extproc.txt>)

Extproc has been found to suffer from another buffer overflow vulnerability. Oracle 10g imposes a length limit on the library name to be loaded by extproc. However, this length limit can be evaded by passing environment variables as part of the library name. Later on the environment variable is expanded allowing the buffer overflow to be exploited. For example '\$PATH' is 5 characters long; this passes the length check. However, when expanded '\$PATH' becomes many more characters. Exploitation depends upon the system setup but by trial and error a balance can be found allowing arbitrary code to be executed. No user ID or password is required to exploit this vulnerability.

3. Clear Text Passwords Disclosure

The 10g Oracle database server may have passwords in clear text in world

[NEWS] Multiple Vulnerabilities in Oracle Database (Character Conversion, Extproc, Password Disclosure, I

readable files. The password for the SYSMAN account (a DBA) can be found in \$ORACLE_HOME/hostname_sid/sysman/config/emoms.properties. This file is world readable.

Also, on installing Oracle 10g if the installer supplies the same password for the SYS, SYSTEM, DBSNMP and SYSMAN accounts and that password has an exclamation mark in it (e.g. f00bar!!) then an error occurs in the DB install when the passwords are set for SYSMAN and DBSNMP.

This error is logged to the "postDBCcreation.log" logging the password:

```
Alter user SYSMAN identified by f00bar!! account unlock ERROR at line 1:  
ORA-00922: missing or invalid option
```

```
Alter user DBSNMP identified by f00bar!! account unlock ERROR at line 1:  
ORA-00922: missing or invalid option
```

This file is world readable giving attackers access to what the passwords are for these powerful accounts. Please note that no error is generated for SYS or SYSTEM and these accounts are assigned the password f00bar!!. The other accounts are given their default passwords.

4. ISQLPlus file access vulnerability

The 10g Oracle Application Server installs ISQL*Plus. Once logged in, an attacker can use load.uix to read files on the server. From isqlplus it is possible to load a script and execute it. On navigating to <http://server:5560/isqlplus/load.uix> two input boxes are displayed – one called "URL" and the other "File". By entering in a full path an attacker can load and read any file that the oracle user can read. For example "/etc/passwd" on Linux or "C:\boot.ini" on windows. An attacker can read the the files mentioned in 'Clear Text Passwords Disclosure' vulnerability above to gain the privileges of SYSMAN.

5. TNS Listener DoS

The 10g Oracle TNS Listener is vulnerable to a denial of service vulnerability. This occurs by sending the Listener a malformed service_register_NSGR request. Byte 182 of the request is used as an offset to a pointer; in a normal request this byte's value is 5 but by setting it to say 0xCC an attacker can get the Listener to access (read) an arbitrary value which causes the Listener to access violate/core dump.

Vendor Status:

A patch (#68) was released for all the problems described above by Oracle. See <<http://metalink.oracle.com/>> <http://metalink.oracle.com/> for more details.

Original Advisories can be found at:

<<http://www.ngssoftware.com/advisories/oracle23122004G.txt>>
<http://www.ngssoftware.com/advisories/oracle23122004G.txt>
<<http://www.ngssoftware.com/advisories/oracle23122004F.txt>>
<http://www.ngssoftware.com/advisories/oracle23122004F.txt>
<<http://www.ngssoftware.com/advisories/oracle23122004F.txt>>
<http://www.ngssoftware.com/advisories/oracle23122004F.txt>
<<http://www.ngssoftware.com/advisories/oracle23122004E.txt>>
<http://www.ngssoftware.com/advisories/oracle23122004E.txt>

eam: [NEWS] Multiple Vulnerabilities in Oracle Database (Character Conversion, Extproc, Password Disclosure, ISQLPlus

<<http://www.ngssoftware.com/advisories/oracle23122004D.txt>>
<http://www.ngssoftware.com/advisories/oracle23122004D.txt>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.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.