

Oracle Database 10g Rel. 2 – Event 10053 logs TDE wallet password in cleartext

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-01/msg00309.html>

- *From:* ak@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 - *Date:* 17 Jan 2006 22:04:52 -0000
-

Name Event 10053 logs TDE wallet password in cleartext
Systems Oracle Database 10g Release 2
Severity High Risk
Category Information disclosure
Vendor URL <http://www.oracle.com/>
Author Alexander Kornbrust (ak at red-database-security.com)
Date 17 January 2005 (V 1.00)
Oracle Bug 5802023
Time to fix 190 days

Details:

#####

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.

Test case:

#####

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

Session altered.

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

System altered.

Test case

Excerpt from trace file ##### [] Current SQL statement for this session:

```
ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY "secretpassword"
```

[]

Excerpt from trace file

Oracle Database 10g Rel. 2 – Event 10053 logs TDE wallet password in cleartext

Patch Information:

#####

Oracle fixed this issue with the patches from the critical patch update january 2006 for Oracle 10g Release 2.

History:

#####

11-jul-2005 Oracle secalert was informed

12-jul-2005 Bug confirmed

17-jan-2006 Oracle published the Critical Patch Update January 2006
(CPU January 2006)

17-jan-2006 Red-Database-Security published this advisory

© 2006 by Red-Database-Security GmbH

http://www.red-database-security.com/advisory/oracle_cpu_jan_2006.html

- Prev by Date: [**Oracle DBMS Access Control Bypass in Login**](#)
- Next by Date: [**Oracle Reports – Read parts of files via desname \(fixed after 874 days\)**](#)
- Previous by thread: [**Oracle DBMS Access Control Bypass in Login**](#)
- Next by thread: [**Oracle Reports – Read parts of files via desname \(fixed after 874 days\)**](#)
- Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)