

# [NEWS] Oracle DBMS Access Control Bypass in Login

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00090.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 25 Jan 2006 10:05:18 +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 DBMS Access Control Bypass in Login

---

## SUMMARY

Oracle is a widely deployed DBMS. Clients use a protocol called TNS to communicate to the Oracle server. Protocol messages are used for session setup, authentication and data transfer. The standard authentication mechanism requires a client to supply a valid pair of user name and password.

During the login process an Oracle user with no more than "create session" privileges can execute commands in the context of the special database user SYS. This of course grants any user the highest administrative privileges possible.

## DETAILS

Vulnerable Systems:

- \* Oracle 8i (8.1.7.x.x)
- \* Oracle 9i (9.2.0.7)
- \* Oracle 10g Release 1 (10.1.0.4.2)
- \* Oracle 10g Release 2 (10.2.0.1.0)

## [NEWS] Oracle DBMS Access Control Bypass in Login

The authentication part of the protocol is comprised of two steps, including two different client requests and two server responses respectively. The first request (message code 0x76) contains only the user name while the second (message code 0x73) contains the user name and an obfuscated password. This second request also contains a list of name-value pairs describing various attributes of the client. The value named "AUTH ALTER SESSION" is intended for setting up session attributes related to the locale and language, in the form of an ALTER SESSION SQL statement. It turns out that this value can contain any SQL statement. Moreover, this command is executed in the context of the SYS user, which operates outside of the Oracle access control mechanism. Thus, by setting the value of "AUTH ALTER SESSION" to an arbitrary SQL statement an attacker can execute any arbitrary command in the database. In particular, the attacker can create a new database account and create DBA privileges to the new account.

Notice that if the attacker tries to execute "GRANT DBA TO attacker\_account" a deadlock occurs and attacker\_account cannot login to the database until the connection is closed.

### Disclosure Timeline:

Vendor notified on 02-Nov-05

Patch released on 17-Jan-06 (5745699 OAUTH – REMOTE AUTHENTICATED ESCALATE TO DBA VIA AUTH ALTER SESSION)

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:shulman@xxxxxxxxxxxx>> shulman.

=====

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@xxxxxxxxxxxxxx

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

=====

=====

### 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.

[NEWS] Oracle DBMS Access Control Bypass in Login

- Prev by Date: [\*\[NT\] TFTPd Filename Format String\*](#)
- Next by Date: [\*\[REVS\] Attacking Automatic Wireless Network Selection\*](#)
- Previous by thread: [\*\[NT\] TFTPd Filename Format String\*](#)
- Next by thread: [\*\[REVS\] Attacking Automatic Wireless Network Selection\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)