

# [Full-disclosure] CVE-2008-2625: Oracle DBMS – Proxy Authentication Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-10/msg00365.html>

---

- *From:* "Amichai Shulman" <[shulman@xxxxxxxxxxx](mailto:shulman@xxxxxxxxxxx)>
  - *Date:* Sun, 19 Oct 2008 08:40:42 +0200
- 

Oracle DBMS – Proxy Authentication Vulnerability

## Background

Oracle is a widely-deployed Database Management System (DBMS) that supports a variety of applications. Many multi-tier applications are designed to use proxy authentication, restricting a middle tier to establish the database connection on behalf of the users. The standard authentication mechanism requires the client, the middle tier in this case, to provide valid credentials in order to authenticate and connect to the DBMS. User sessions are then created through the proxy connection. Oracle TNS protocol messages are used for session setup, authentication and data transfer.

## Scope

Imperva's Application Defense Center (ADC) conducts extensive research on enterprise applications and databases. During its research, the team has identified a vulnerability in Oracle's proxy authentication and access control mechanism.

## Findings

While proxy authentication is enabled for a user account through a proxy account, it is possible to create a separate connection using the original user account without authenticating the connection.

## Details

Oracle supports a proxy authentication mode which a user establishes a session through a proxy and the proxy establishes a session on the user's behalf to the database. These sessions are created using the Oracle TNS protocol level messages and do not require additional authentication. This scenario is recommended by Oracle for multi-tier environments.

While the user sessions are open through the proxy connection, an attacker can create a new connection to the database impersonating the original user without supplying a password. The attacker executes the attack by opening a TNS connection to the database server and sending a manipulated authentication message with the login mode flags set to proxy login and the session ID and serial number of the original session opened through the proxy account.

#### Vulnerability ID

Proposed CVE Candidate (as of October 14, 2008): CVE-2008-2625

#### Tested Versions

##### Vulnerable

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)

#### Vendor's Status

Vendor notified on December 13, 2005. Patch released by vendor on October 14, 2008.

#### Workaround

- \* Always require password authentication, even for proxy connections
- \* Alternatively, disable proxy authentication mode and enforce this policy by configuring the SecureSphere Database Security Gateway to alert when users are granted proxy access
- \* The SecureSphere Database Security Gateway can also enforce all proxy account connections to the database originate from the proxy

[Full-disclosure] CVE-2008-2625: Oracle DBMS – Proxy Authentication Vulnerability

server IP address

Discovered by:

Amichai Shulman – Imperva Co-Founder, CTO and Head of Imperva's Application Defense Center (ADC).

Disclaimer

The information within this advisory is subject to change without notice. Use of this information constitutes acceptance for use in an AS IS condition. Any use of this information is at the user's own risk. There are no warranties, implied or expressed, with regard to this information. In no event shall the author be liable for any direct or indirect damages whatsoever arising out of or in connection with the use or spread of this information.

Copyright (c) 2007 Imperva, Inc.

Redistribution of this alert electronically is allowed as long as it is not edited in any way. To reprint this alert, in whole or in part, in any medium other than electronic medium, [adc@xxxxxxxxxxx](mailto:adc@xxxxxxxxxxx) for permission.

Amichai Shulman  
CTO

125 Menachem Begin St.  
Tel Aviv 67010  
Israel

(972) 3-6840103 Office  
(972) 54-5885083 Mobile  
(972) 3-6840200 Fax  
[shulman@xxxxxxxxxxx](mailto:shulman@xxxxxxxxxxx)

Download Scuba by Imperva  
FREE Database Assessment Scanner  
[www.imperva.com/scuba](http://www.imperva.com/scuba) <blocked:<http://www.imperva.com/scubam>>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>