# Potential Vulnerabilities in Oracle Internet Application Server

## Versions Affected:

The first potential vulnerability is found in the WebDB/Portal component of Oracle Internet Application Server (iAS) Listener and modplsql, up to and including release 3.0.7 (associated modplsql version is 3.0.0.8.1). The second potential vulnerability affects all versions of the PL/SQL gateway including Oracle Application Server (OAS), the WebDB/Portal listener, and iAS.

## Platforms Affected:

All platforms.

## Description:

The first possible vulnerability is essentially a configuration issue associated with the Portal Listener and modplsql. When these are installed, the default configuration allows all users access to the Listener and modplsql administration pages.

A second potential vulnerability may occur if customers grant public access to PL/SQL procedures, in particular those which access an Oracle database such as OWA, SYS and DBMS. Since publicly accessible procedures may be accessed through a URL, it may be possible to invoke these procedures through a URL and cause SQL statements to be executed on a back-end Oracle database.

## Likelihood of Occurrence:

The first vulnerability may occur if the default permission for admin pages is not changed after WebDB/Portal install. The second vulnerability depends on the design of applications which use the PL/SQL gateway, but may occur whenever procedures are granted public access.

## Possible Symptoms:

The first vulnerability may allow unauthorized access to administrative pages. The second vulnerability may allow unauthorized access to data within a back-end Oracle database.

## Workaround:

The workaround for the first vulnerability is to specify that the Listener and modplsql administrator must be one or more known users. This may be done by simply editing the wdbsvr.app configuration file on WebDB/Portal. All versions of the Listener and modplqsl use this file; at the top of the file is a setting entitled 'administrators='. Customers should set this property to specify one or more named users who are allowed to have administrative privileges.

In addition, customers can change the path used to reference the admin pages. By default this path is 'admin_', but can be changed in the wdbsvr.app file to something else (e.g., changing it to 'foo' would change the admin page URL to http://<server>:<port>/pls/foo/gateway.htm).

Customers who have granted public access to PL/SQL procedures on WebDB/Portal can mitigate the risk associated with second vulnerability in two ways.

The first is to revoke public access to procedures such as OWA, SYS and DBMS which can potentially execute user-specified SQL statements.

For modplsql in iAS, a second solution is to disable access to URLs which match certain criteria. For example, in the case of SYS, OWA, and DBMS this may be done by adding the following rules to the plsql.conf file:

```
# Disallow direct access to any PL/SQL procedure in the SYS schema, in particular
sys.dbms_job:
<Location /pls/*/sys.*>
  SetHandler pls_handler
  Order deny,allow
  Deny from all
</Location>

# Disallow direct access to any DBMS* PL/SQL procedure which is called thru public synonyms:
<Location /pls/*/dbms*>
  SetHandler pls_handler
  Order deny,allow
  Deny from all
</Location>

# Disallow direct access to any owa_util procedure:
<Location /pls/*/owa_util.*>
  SetHandler pls_handler
  Order deny,allow
  Deny from all
</Location>
```

Note that since Apache treats these rules as case sensitive, the first rule prevents access to any URL including sys.*, but would allow access to URLs with SYS.* or Sys.*.  It may be therefore be necessary to include additional rules with different case combinations in the names of the procedures (e.g., repeat rule 1 in the config. file, substituting SYS.*, Sys.*, etc. for sys.*).

Note also that the plsql.conf file can be configured to include rules which prevent access to URLs containing specific SQL statements such as select, insert, grant, etc., keeping in mind that rules are case sensitive.

**Patches:**
Release 3.0.8 of Portal will restrict default access to the Listener and modplsql admin pages on installation.

Oracle is developing enhancements for iAS which will allow customers to define case insensitive rules to disable access to certain procedures via URL.