Oracle Security Alert #61
Dated: 3 November 2003
Updated 13 November 2003
Severity: 1

SQL Injection Vulnerability in Oracle9*i* Application Server

Description

A potential security vulnerability has been discovered in the Portal component of Oracle9*i* Application Server, Release 9.0.2. A knowledgeable, malicious and unauthenticated user can potentially inject a SQL script through a URL in order to gain unauthorized access to user data in Oracle9*i* Application Server.

Products Affected

- Oracle9*i* Application Server Portal Release 1, v 3.0.9.8.5 (and earlier)
- Oracle9*i* Application Server Portal Release 2, v 9.0.2.3.0 (and earlier)

Portal version 9.0.2.6 and onwards are not vulnerable.

Components affected (where applicable to the product version):

- List of Values (LOVs)
- Portal DB Provider Forms
- Portal DB Provider Hierarchy
- Portal DB Provider XML component

Platforms Affected

See Patch Availability Matrix.

Required conditions for exploit

An unauthenticated user with HTTP access. Note that Portal is installed by default with Oracle9*i* Application Server.

Risk to exposure

Risk to exposure is high. A SQL injection attack via the Internet is, in Oracle's opinion, likely if the required conditions listed above are met. This vulnerability is also susceptible to an insider attack originated on the corporate Intranet. An unauthenticated user can submit unauthorized SQL queries on the Oracle9*i* Application Server Data Dictionary tables and/or also submit costly (time consuming) queries that may affect the performance of Oracle9*i* Application Server.

How to minimize risk

It is not feasible to disable public access from the vulnerable components to mitigate the risk. Oracle strongly recommends that the patches identified in this alert be applied.

Follow Oracle's best practices for database and application server:

http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf
http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
http://otn.oracle.com/deploy/security/oracle9iAS/

and investigate typical IT deployments of firewalls, etc.

Ramification for customer

Oracle strongly recommends applying the patch for this potential vulnerability.

Oracle recommends that customers review the severity rating for this Alert and patch accordingly. See

http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf

for a definition of severity ratings.

Patch Information

The patch is platform independent and may be applied across all platforms on which Portal is supported.

Oracle E-Business Suite Release 11i customers

Release 11i customers **must not** apply Portal 3.0.9.8.5 or its associated patches listed in the **Patch Availability Matrix** to existing environments.

- For all Release 11i customers using Portal 3.0.9.8.4:

  Patch **3237913** is available for download from Metalink for Release 11i customers using Portal 3.0.9.8.4.

- For all Release 11i customers using earlier versions of Portal:

  Existing Release 11i environments running earlier versions of Portal (e.g. Portal 3.0.9.8.2) must be upgraded to Portal 3.0.9.8.4 prior to applying Patch **3237913**.

- For Release 11i customers with environments created with the 11.5.7 and higher Rapid Installs, and who are not using Portal:

  Portal 3.0.9 schemas were delivered as part of the Rapid Install and may be vulnerable. It is recommended that the Portal schemas be deinstalled following the procedures in Chapter 2.7.1, "Deinstalling a Single Oracle Portal Schema or the Login Server" of the "Oracle9iAS Portal Configuration Guide Release 3.0.9 (Part Number A90096-01)". Deinstallation of the Login Server schemas is not required. This documentation is available on the Oracle Technology Network:

  http://download-west.oracle.com/docs/cd/A97335_01/portals.102/a90096/cgpost.htm#1001575

- For Release 11i customers with environments created with the 11.5.1 to 11.5.5 Rapid Installs, and who are not using Portal:

  Portal 3.0.9 schemas were not delivered as part of the Rapid Install for these releases. No action is required.

Fixed by

An interim (one-off) patch for this issue is available for the following Oracle 9*i*AS Portal versions:

- Oracle9*i* Application Server Portal Release 1, v 3.0.9.8.5
- Oracle9*i* Application Server Portal Release 2, v 9.0.2.3.0

Download the appropriate one-off patch from the Oracle Support Services web site, Metalink (http://metalink.oracle.com).

1. Click on the **Patches** button.
2. Click on "Simple Search".
3. In the "Search By" option, select 'Patch Number(s)' from the drop-down menu, and enter the patch number from the Patch Availability Matrix in the box.
4. Select the platform.
5. Click on the “Go” button.
6. Click on the “Download” button.
7. Recommended: you should also click on the “View README” button for additional information and instructions.

Please review Metalink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable.

Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Patch Availability Matrix

Platforms	Product Version	Portal Version	Patch Number
All	E-Business 11i	3.0.9.8.4	3237913
All	iAS 1.0.2.2	3.0.9.8.5	3068980
All	iAS 9.0.2.1	9.0.2.3	2853895
All	iAS 9.0.2.2	9.0.2.3A	2853895
All	iAS 9.0.2.3	9.0.2.3B	2853895

Note:

- The 'A' and 'B' suffixes only serve to distinguish the labels used to release the Portal code with the bundled Oracle 9*i*AS patchset. This is the version that must be patched with the referenced patch number.
- Patch 2853895 listed under Oracle 9*i*AS version 9.0.2.0 on Metalink is an obsolete duplicate. Please obtain the patch that is listed against 9*i*AS version 9.0.2.1.
- In order to apply the patch, you must first upgrade to Oracle9*i* Application Server Portal, Release 2, v9.0.2.3.0, if on Release 2, or to Oracle9i Application Server Portal, Release 1, v3.0.9.8.5, if on Release 1.
- For more information on Portal, please see http://portalcenter.oracle.com/upgrades

Credits

Oracle Corporation thanks David Litchfield, of Next Generation Security Software Ltd., for discovering and promptly bringing this potential security vulnerability to Oracle's attention. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/advisories.html.

Modification History

03-NOV-03: Initial release, version 1
07-NOV-03: Updated for E-Business Suite, version 2
13-NOV-03: Updated for availability of E-Business Suite patch and clarification of schema deinstallation, version 3