Vulnerability in Oracle E-Business Suite Release 11i Applications Desktop Integrator

Overview

A potential security vulnerability has been discovered in Applications Desktop Integrator (ADI) version 7.X for Oracle E-Business Suite Release 11i. A debug version of the FNDPUB11I.DLL was inadvertently released with a patch to Applications Desktop Integrator (ADI) version 7.X. This DLL writes a debug file to the client machine that includes the clear text APPS schema password. A malicious user could use this DLL to obtain the APPS schema password and thereby gain elevated privileges.

Products Affected

Any Oracle E-Business Suite Release 11i installation may be affected by this vulnerability, even if the ADI product is not being used.

Platforms Affected

All platforms.

Solution

The debug version of FNDPUB11I.DLL has been replaced with a production version. In addition, a patch is available that introduces an enhanced security feature, Application Server Security, to prevent the debug DLL from connecting to the database. The complete solution to this vulnerability requires *both* replacement of the debug version DLL and implementation of the Application Server Security patch.

The patches for this vulnerability can be downloaded from the Oracle Worldwide Support Services web site, Metalink (http://metalink.oracle.com). Press the "Patches" button to get to the Patch Download page. Click on the link labeled "Click Here for ALL Product Patches". Enter the patch number, select a platform, then press Submit to access the correct patch for your platform.

To obtain the full Application Server Security patch, download patch 1779336. The patch includes:

- Application Server Security feature
- Trusted implementations of middle-tier connection code

If you do not wish to upgrade your middle-tier application servers at this time**,** a database-only version of the patch is also available as Patch Number 1785034. This patch contains only the Application Server Security feature. As a result of applying this patch, application servers with old connection code will need to be registered as trusted servers before they can access the database. See the README.TXT files associated with the patch for further instructions.

Apply the Application Server Security patch and turn server security 'ON'. The old versions of ADI will no longer be able to connect. New versions of ADI are available which contain a trusted implementation of the FNDPUB11I.DLL connection code. A new version of ADI will be required to connect to a database which has Application Server Security enabled. Obtain the correct ADI patch for your current version:

ADI Version	**Patch**
7.0	1775480
7.1.2	1775479
7.1.3	1775476

After turning on Application Server Security, it is strongly recommended that the APPS schema password be changed.

Credits

Oracle Corporation wishes to thank Melanie Abbas for discovering this vulnerability.