Vulnerability in Launch of Forms from Oracle E-Business Suite

Overview
A potential security vulnerability has been discovered in Oracle E-Business Suite Release 11i. This vulnerability may allow a knowledgeable and malicious user to launch Forms-based Applications under the identity of another user.

Description
A user successfully authenticating to Oracle Applications is connected to a URL specific to his session that launches Oracle Forms. The URL is valid as long as the user is logged into his E-Business session, or the session has not timed out. A malicious user who has access to the PC of an authorized user can obtain the exact URL used to launch Forms for the authorized user's session, and can then access that URL from another PC. Since physical presence (or "shoulder surfing") at another user's PC is required to exploit the vulnerability, the likelihood of occurrence is low and can be managed with the following operational procedures:

- When exiting an E-Business session, a user should log out through the personal home page Logout button. Simply closing the browser does not force a logout, and will leave the user session active.

- When leaving his or her PC unattended, a user should lock the screen.

Products Affected
Oracle E-Business Suite Release 11i (Releases 11i.1 - 11i.4)

Platforms Affected
All

Patch Solution
Apply Application patch for bug 1739272. This patch closes the vulnerability by providing a secure, session-specific token in addition to the session URL, which is used to ensure that only the authenticated and authorized user can access the URL specific to his session. Malicious users cannot access another user's session by typing in the URL, since the malicious user does not have the correct token for the session.

The patch for this vulnerability can be downloaded from the Oracle Worldwide Support Services web site at
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 1739272 as the Patch Number, select a Platform, then press Submit.