Oracle Security Alert 56
Dated: July 23, 2003
Severity: 1

Buffer Overflow Vulnerability in Oracle E-Business Suite

Description

A potential security vulnerability has been discovered in Oracle E-Business Suite. The FNDWRR CGI program is vulnerable to malformed requests that may permit a knowledgeable and malicious user to cause the FNDWRR executable to crash. However, this crash will neither result in a Denial of Service (DoS) against Oracle E-Business Suite, nor prevent the FNDWRR executable from reliably serving correctly formed requests, but it may grant a user unauthorized access to Oracle E-Business Suite.

Products Affected

- Oracle E-Business Suite 11i, Release 1 through Release 8
- Oracle Applications, All Releases

Platforms Affected

All platforms.

Required conditions for exploit

User with HTTP access to a Web Server set up to spawn the FNDWRR CGI program.

Risk to exposure

Risk to exposure is high, as any user with HTTP access and specialized knowledge can exploit this vulnerability over the Internet to gain unauthorized access to Oracle E-Business Suite if the conditions mentioned above are met.

How to minimize risk

There are no workarounds that can directly address this potential security vulnerability, but a patch is available (see below). Oracle strongly recommends that customers follow best practices for Oracle E-Business Suite, Metalink note 189367.1 "Best Practices for Keeping Your E-Business Suite Secure" available at http://metalink.oracle.com.

Ramification for customer

Customers are vulnerable unless the patch is applied.

Oracle strongly 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 enhances the robustness of the FNDWRR CGI program.

Fixed by
Obtain and install the correct Mandatory Applications Security Patch for your release of E-Business Suite:

- Oracle E-Business Suite 11i, Releases 1 through 8
- Oracle Applications, All Releases

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

1. Click on the Patches button.
2. Click on the "New Metalink Patch Search ".
   If you are not on the "Simple Search" screen, click on the "Simple Search" button.
3. Input the bug number 2919943 on the "Search by Patch Number" box.
4. Click Go.
5. Select the patch for the appropriate product version.
6. Select the appropriate platform.
7. Click Download.

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	Oracle E-Business Suite 11i Releases 1-8	Oracle Applications, All Releases
Sun Solaris Intel (32-bit)	N/A	2919943
Sun Solaris SPARC (32-bit)	2919943	2919943
IBM AIX 4.3.3 and 5L (32-bit)	2919943	2919943
MS Windows NT/2000/XP	2919943	2919943
HP-UX (32-bit)	2919943	2919943
HP Tru64	2919943	2919943
LINUX	2919943	N/A
SGI 32-bit UNIX	N/A	2919943

N/A: The Oracle E-Business Suite Release/Version is not available for this platform.

Planned: The patch is not released yet. Future release (e.g. 11.5.9 and higher) of the Oracle E-Business Suite will contain the fix by default.

Credits
Oracle Corporation thanks Stephen Kost of Integrigy Corporation for discovering and promptly bringing this potential security vulnerability to Oracle's attention. The Integrigy alert is available at http://www.integrigy.com/alerts.htm.

Modification History
23-JUL-03: Initial release, version 1