Oracle Security Alert #45
Dated: 04 October 2002 (Updated: 20 May 2004)
Severity: 1

Security Release of Apache 1.3.27

Description
Apache has released version 1.3.27 of its HTTP Server that contains fixes for the security vulnerabilities noted below and described at http://cve.mitre.org. The vulnerabilities that affect all of the supported versions of the Oracle HTTP Server (OHS) are:

1. CAN-2002-0839: This is a security vulnerability involving System V shared memory based scoreboards. It can only occur on Oracle Linux and HP ports. Exploitation of this vulnerability requires that a malicious and knowledgeable user be able to run his programs on the server web site. As few commercial web sites allow this, the vulnerability applies to few sites. If a malicious and knowledgeable user is able to run his own programs, the web site has more serious, unrelated security issues than the exploit of this vulnerability.

2. CAN-2002-0840: This is a cross-site scripting vulnerability involving the default error 404 pages. It can occur on all Oracle database platforms. Exploitation of this vulnerability requires the use of wildcard DNS and the setting of UseCanonicalNames = OFF.

3. CAN-2002-0843: There were potential buffer overflows in Apache Bench (ab) that could be exploited by a malicious server. Note that 'ab' is not in Apache itself but is an HTTP client utility used for generating load for performance testing. This vulnerability only occurs when the 'ab' load generating HTTP client, used for performance testing, is used against a malicious HTTP server.

These security vulnerabilities are described in more detail at http://cve.mitre.org/

Products affected
OHS in Oracle Database Releases 8.1.7.x, 9.0.1.x and 9.2.x
OHS in Oracle9*i* Application Server Releases 1.0.2.x and 9.0.2.x

E-Business Suite 11i
The Oracle E-Business Suite11i uses several components delivered as part of theOracle9i Application Server Release 1 (v 1.0 and v 1.0.2.2). Oracle E-Business Suite11i customers may be impacted by the security alerts issued for v 1.0.2.2. If you are an Oracle E-Business Suite 11i customer, please make sure that you have applied the latest ROLLUP PATCH for Oracle9i Application Server Release 1, v 1.0.2.2 & Oracle E-Business Suite 11i as mentioned in the document entitled "Installing Oracle9i Application Server with Oracle E-Business Suite 11i", (Metalink Note146468.1).

Platforms affected
All except as noted in item #1 in the Description above.

Workarounds
There is no workaround for CAN-2002-0839.

There are workarounds for CAN-2002-0840 and application of any or all of these workarounds will mitigate risk of exposure to CAN-2002-0840. Oracle strongly recommends the following workaround:

1. Set a custom 404 error page.
2. Disable wildcard DNS.
3. Set the following parameter: UseCanonicalNames = ON.

There is a workaround for CAN-2002-0843: Oracle strongly recommends not using 'ab' to generate load against unknown HTTP servers to protect against the vulnerability described in CAN-2002-0843.

Patch Information
Oracle has fixed the vulnerabilities described in CAN-2002-0839 and CAN-2002-0840 in patch number **2611482** for all supported versions of OHS on all platforms except as noted in item #1 (in the Description).

No patch will be generated for general distribution for the vulnerabilities described in CAN-2002-0843. If you believe that you do need this HTTP load generating ability against unknown HTTP servers, please contact Oracle Worldwide Support Services for special distribution of 'ab'.

Download currently available patches from Oracle Worldwide Support Services web site, Metalink, (http://metalink.oracle.com). Activate the 'Patches' button to get to the patches web page. Enter Patch Number **2611482** as indicated above and activate the 'Submit' button.

Note that Patch Number **2424256** must be applied prior to applying Patch Number **2611482.**

Please review Metalink or check with Oracle Worldwide Support Services periodically for patch availability if the patch for your platform is unavailable. Please check the matrix provided below for status and details on patch availability.

Please note that Oracle does not intend to release a patched version of OHS with version number 1.3.27.

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 that patch.

Patch Matrix

Release	**DBMS**	***i*AS**	***i*AS**	***i*AS**	**DBMS**	**DBMS**	***i*AS**	***i*AS**	***i*AS**	***i*AS**
Platform	**9.2.0.0**	**9.0.3.0**	**9.0.2.1**	**9.0.2.0.1**	**9.0.1.0**	**8.1.7.0**	**1.0.2.2**	**1.0.2.1S**	**1.0.2.1**	**1.0.2.0**
Solaris-32(453)	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct
AIX(319)	N/A	N/A	N/A	N/A	N/A	01-nov	01-nov	01-nov	01-nov	01-nov
NT/2000(912/100)	14-oct	N/A	N/A	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct	14-oct
HPUX(2)	N/A	N/A	N/A	N/A	N/A	25-oct	25-oct	25-oct	25-oct	25-oct
TRU-64(87)	01-nov	N/A	N/A	01-nov	01-nov	01-nov	01-nov	01-nov	01-nov	01-nov
LINUX(46)	25-oct	N/A	15-oct	25-oct	25-oct	25-oct	25-oct	25-oct	25-oct	25-oct
AIX64(38)	01-nov	N/A	N/A	01-nov	01-nov	NR	NR	NR	NR	NR
HP-64(59)	25-oct	N/A	N/A	01-nov	25-oct	NR	NR	NR	NR	NR

NR = Not Released – for example 9021 is not released on 32-bit AIX or HP
N/A = Not Applicable – for example Linux 9030 has the fixes built in, so no patch is required