Oracle Security Alert #45
Dated: 04 October 2002 (Updated: 08 October 2002)
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.miter.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

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
Patches for the vulnerabilities described in CAN-2002-0839 and CAN-2002-0840 will be released against bug 2611482. Patches will be available on Metalink, http://metalink.oracle.com, for all

supported versions of OHS on all platforms except as noted in item #1 (in the Description). A matrix of patch release dates for these platforms will be provided on Thursday, October 10, 2002.

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'.

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 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.