Oracle Security Alert 66
Dated: 12 March 2004
Updated: 12 March 2004
Severity: 1

Vulnerabilities in Oracle Application Server Web Cache

Description

Security vulnerabilities have been discovered in Oracle Application Server Web Cache 10*g* (9.0.4.0.0) and Oracle9*i* Application Server Web Cache.

Supported Products Affected

- Oracle Application Server Web Cache 10*g* (9.0.4.0.0)
- Oracle9*i*AS Web Cache 9.0.3.1.0
- Oracle9*i*AS Web Cache 9.0.2.3.0
- Oracle9*i*AS Web Cache 2.0.0.4.0

Platforms Affected

All Oracle supported platforms - Sun Solaris, HP/UX, HP Tru64, IBM AIX, Linux and Windows.

The only exception is Oracle Application Server Web Cache 10*g* (9.0.4.0.0) on Windows, Tru64 and AIX (release pending), which already contain fixes that are described in the Patch Availability Matrix.

E-Business Suite 11*i* customers using Oracle iStore 11*i* (11*i*.IBE.O and later) with Oracle Web Cache 9.0.2.2 (as described in Certify Issue 382345) must apply corresponding patch(es) specified in the Patch Availability Matrix.

E-Business Suite 11*i* Early Adopter customers implementing MetaLink note 233436.1 **Installing Oracle Application Server 10*g* with Oracle E-Business Suite Release 11*i*** must apply corresponding patch(es) specified in the Patch Availability Matrix for Oracle Application Server 10*g* (9.0.4.0.0).

Note that Oracle9*i*AS Web Cache 2.0.0.4.0 is part of the Oracle9*i*AS Release 1 (1.0.2.2.0).

See the Patch Availability Matrix for details.

Required conditions for exploit

Web Cache must be running and configured to listen on the Oracle Application Server Web Cache listener port for any client request, regardless of the type of origin Web server (for example, Oracle HTTP Server, Apache or other web servers). If the client request is sent directly to origin Web server (i.e. Oracle HTTP Server, Apache or others), bypassing Web Cache, these vulnerabilities cannot be exploited.

Note that a typical Core or Mid-Tier default installation of Oracle Application Server includes Web Cache. Web Cache is also available as a standalone install.

Risk to exposure
Risk to exposure to the vulnerabilities is high. Firewalls deployed within a corporate Intranet or between a corporate Intranet and the Internet do not protect against these vulnerabilities.

How to minimize risk
There is no workaround that fully addresses these vulnerabilities. Oracle strongly recommends applying the patches identified in this Alert as soon as possible, restricting or carefully monitoring access to Web Cache.

Ramification for customer
Oracle Corporation strongly recommends that customers review the severity rating of this Alert and patch accordingly. See http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf for a definition of severity ratings.

Patch Availability

Please see MetaLink Document ID 265310.1 (http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=265310.1) for the patch download procedures and for the Patch Availability Matrix for this Oracle Security Alert.

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.

Modification History

12-Mar-04: Initial Release, Version 1