

[NEWS] Webcache Client Requests Bypass OHS mod_access Restrictions

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0162.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/27/05

To: list@securiteam.com

Date: 27 Apr 2005 19:07:58 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Webcache Client Requests Bypass OHS mod_access Restrictions

SUMMARY

A vulnerability in Oracle's Webcache allows attackers to access protected URLs by using webcache.

DETAILS

Vulnerable Systems:

* Oracle Application Server version 10.x – OHS version 1.0.2

Example:

(Port 7778 = Webcache, Port 7779 = OHS)

The following URLs are NOT protected if you access them via the Webcache server:

http://server01:7778/dmsoc4j/AggreSpy?format=metrictable&nountype=ohs_child&orderby=Name

<http://server01:7778/server-status>

<http://server01:7778/dms0>

The following URLs are protected if you access them via the OHS server:

http://server01:7779/dmsoc4j/AggreSpy?format=metrictable&nountype=ohs_child&orderby=Name

Securiteam: [NEWS] Webcache Client Requests Bypass OHS mod_access Restrictions

http:// server01:7779/server-status
http:// server01:7779/dms0

Workaround:

Add "UseWebCacheIP ON" to Oracle's httpd.conf configuration file.

Patch:

Oracle addressed this issue by introducing the parameter "UseWebcacheIP" to the Oracle HTTP Server(OHS).

References:

<http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=263943.1>
http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=263943.1

Disclosure Timeline:

01-oct-2003 Oracle secalert was informed
01-oct-2003 Bug confirmed
26-apr-2005 Red-Database-Security published this advisory

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:ak@red-database-security.com>> Kornbrust, Alexander.

The original article can be found at:

<http://www.red-database-security.com/advisory/oracle_webcache_bypass.html>
http://www.red-database-security.com/advisory/oracle_webcache_bypass.html

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.